ห้ามจำหน่าย

แนวปฏิบัติของสำนักงานสอบบัญชี ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

(ฉบับสมบูรณ์)

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

ฉบับปรับปรุง ตุลาคม 2566

คำนำ

คณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ภายใต้สภาวิชาชีพบัญชี ในพระบรมราชูปภัมภ์ และ PDPA Thailand ได้เล็งเห็นว่ากระบวนการดำเนินการของสำนักงานสอบบัญชีมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นอย่างมากซึ่งผู้ประกอบการสำนักงานสอบบัญชีอาจมีประเด็นปัญหาในทางปฏิบัติในการดำเนินการเพื่อให้เป็นไปตามหลักเกณฑ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติดังกล่าว จึงได้ศึกษาวิจัยเพื่อจัดทำแนวปฏิบัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล ว่าด้วย สำนักงานสอบบัญชี เพื่อเป็นแนวปฏิบัติที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ประกอบการสำนักงานสอบบัญชี สามารถนำไปเป็นแนวปฏิบัติพื้นฐานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างถูกต้องและเหมาะสม

คณะผู้จัดทำหวังเป็นอย่างยิ่ง แนวปฏิบัติของสำนักงานสอบบัญชี ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะสร้างการตระหนักรู้และสร้างการตื่นตัวในวิชาชีพบัญชี รวมทั้งเกิดประโยชน์แก่ผู้ประกอบการสำนักงานสอบบัญชีและลูกจ้างของไทย ที่จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้จริง

คณะผู้จัดทำ

คณะผู้จัดทำ

แนวปฏิบัติของสำนักงานสอบบัญชี ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

คณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. นายปิยะพงศ์	แสงภัทราชัย	ประธานคณะทำงาน
2. นายเสถียร	วงศ์สนันท์	คณะทำงาน
3. นางสาวกุลธิดา	ภาสุรกุล	คณะทำงาน
4. นางวาสนา	สกนธ์ธัญลักษณ์	คณะทำงาน
5. นางสาวอังคศิริ	ทักษ์ธนาคม	คณะทำงาน
6. นางสาวสุภาณี	ศรีสถิตวัตร	คณะทำงาน
7. นายกนกศักดิ์	สุขวัฒนาสินิทธิ์	คณะทำงาน
8. นางอัญชลี	มณีท่าโพธิ์	คณะทำงาน
9. นางสาวเพชรรัตน์	อวยพรส่ง	คณะทำงาน
10. นายสายชล	เชื้อทหาร	คณะทำงาน
11. นางสาวสุธีรา	หงษ์มณี	คณะทำงานและเลขานุการ

คณะทำงานจาก PDPA Thailand

1. ดร.อุดมธิปก	ไพรเกษตร	ที่ปรึกษาอาวุโส
2. คุณสุกฤษ	โกยอัครเดช	ที่ปรึกษาอาวุโส
3. คุณมยุรี	ชวนชม	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
4. คุณสุพิชญา	เอกยะติ	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
5. คุณทรงพล	หนูบ้านเกาะ	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
6. คุณกนกพร	วังศเมธีกูร	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
7. คุณอุมาภรณ์	ไตรตรัสธรรม	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
8. คุณพัชรานันต์	ยิ้มสำราญ	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
9. คุณนภัสสรณ์	วุฒิโรจน์รังษี	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
10. คุณปิยพร	ภู่ประเสริฐ	ที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล
11. คุณลาภิสรา	แสงซื่อ	ผู้ประสานงาน
12. คุณณัฐกานต์	ระถี	ผู้ประสานงาน

องค์กรวิชาชีพ

1. สมาคมสำนักงานสอบบัญชีไทย
2. สมาคมสำนักงานบัญชีคุณภาพ
3. สมาคมสำนักงานบัญชีไทย

สารบัญ

บทที่ 1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 1

1.1 ขอบเขตการบังคับใช้ 1

1.2 นิยามข้อมูลส่วนบุคคล 4

1.3 หลักการในการประมวลผลข้อมูลส่วนบุคคล 5

1.5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 16

1.6 ความรับผิดและบทกำหนดโทษ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 22

บทที่ 2 แนวทางการดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับสำนักงานสอบบัญชี 25

บทที่ 3 แนวทางด้านกระบวนการรองรับการใช้สิทธิ และ การบริหารจัดการเหตุการละเมิดข้อมูลส่วนบุคคล 33

3.1 แนวทางการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล 33

3.2 แนวทางการแจ้งเหตุข้อมูลรั่วไหล (Data Breach Management) 42

บทที่ 4 แนวทางด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 49

บทที่ 5 แนวทางในการจัดทำเอกสารเพื่อการปฏิบัติตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคล 56

5.1 บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities) 57

5.2 ประกาศความเป็นส่วนบุคคล (Privacy Notice) 63

5.3 หนังสือขอความยินยอม (Consent Form) 70

5.4 แบบคำขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request) 72

5.5 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) 74

5.6 หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Notifications) 82

บทที่ 1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act : PDPA ได้ประกาศในราชกิจจานุเบกษา ในวันที่ 27 พฤษภาคม พ.ศ. 2562 และมีผลบังคับใช้กฎหมายทั้งฉบับอย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ซึ่งกฎหมายดังกล่าวได้รับอิทธิพลและหลักการหลายประการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจาก General Data Protection Regulation: GDPR ของสหภาพยุโรป โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ตราขึ้น บนเจตนารมณ์เพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชนในสภาวการณ์ที่การใช้งานข้อมูลส่วนบุคคลกลายเป็นเรื่องที่จำเป็นและมีความสำคัญในทุกภาคส่วนไม่ว่าจะเป็นหน่วยงานภาครัฐหรือองค์กรธุรกิจภาคเอกชน และกฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้กำหนดหลักเกณฑ์ กลไกรวมถึงมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่บทบัญญัติจะมุ่งเน้นสร้างความตระหนักรู้ การออกแบบ ทบทวน และกลไกในการพิจารณาเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต่าง ๆ เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวภายใต้กฎหมาย

1.1 ขอบเขตการบังคับใช้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีลักษณะเป็นกฎหมายกลาง บังคับใช้ครอบคลุมการดำเนินการของบุคคลหรือองค์กรใด ๆ ที่ทำการประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือองค์กรบางประเภทอาจอยู่ภายใต้บังคับของกฎหมายเฉพาะ ซึ่งมาตรา 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดขอบเขตการบังคับใช้กรณีที่มีกฎหมายเฉพาะอื่นบัญญัติไว้เฉพาะว่า ในกรณีที่มีกฎหมายบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษ ให้บังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(2) กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน และ/หรือ มีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมาย

ดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วแต่กรณี

อย่างไรก็ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในเชิงพื้นที่ไว้ตามมาตรา 5 ซึ่งมีขอบเขตการบังคับใช้ ดังต่อไปนี้

1. ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (การประมวลผล) โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งภาครัฐและเอกชนซึ่งอยู่ในราชอาณาจักร ไม่ว่าการประมวลผลนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

2. กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร จะใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร โดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 นั้นยังจำกัดขอบเขตการบังคับใช้กฎหมายไม่ให้ใช้บังคับแก่กิจการ องค์กร หรือกิจกรรมบางประเภท ดังต่อไปนี้

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภา ผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

5. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากนี้ ได้มีกฎหมายลำดับรองกำหนดให้ในบางกรณีนั้น ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อาจจะไม่ต้องปฏิบัติตาม PDPA ในหมวด 2 เรื่องการคุ้มครองข้อมูลส่วนบุคคลและหมวด 3 เรื่องสิทธิของเจ้าของข้อมูล หากเข้าหลักเกณฑ์ตามที่กฎหมายกำหนดไว้ ซึ่งก็คือ “พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บางส่วนมาใช้บังคับ พ.ศ.2566”

โดยกฎหมายลำดับรองฉบับนี้ ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลทั้งภาครัฐและภาคเอกชนได้รับยกเว้นในการปฏิบัติตามหมวด 2 และหมวด 3 ในกรณีดังต่อไปนี้

(1) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการทุจริต เช่น ป.ป.ช. ป.ป.ท. หรือหน่วยงานรัฐที่คณะกรรมการประกาศกำหนด

(2) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจาก กรมสรรพากร กรมศุลกากร หรือกรมสรรพสามิต ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีอากรและความร่วมมือระหว่างประเทศเกี่ยวกับภาษี

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้ และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(3) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากองค์กรปกครองส่วนท้องถิ่นที่คณะกรรมการประกาศกำหนด ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(4) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากสำนักเลขาธิการคณะรัฐมนตรีเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการสถาปนาสมณศักดิ์ การแต่งตั้งหรือถอดถอนข้าราชการ บุคคลหรือคณะบุคคล ซึ่งเป็นพระราชอำนาจของพระมหากษัตริย์

หรือที่ต้องเสนอคณะรัฐมนตรี และการขอพระราชทาน หรือเรียกคืนเครื่องราชอิสริยาภรณ์ ฎีกาซึ่งมีผู้ทูลเกล้าฯถวาย หรือการขอพระราชทานพระมหากรุณาในเรื่องต่าง ๆ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(5) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจเพื่อดำเนินการตามวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญตามที่คณะกรรมการประกาศกำหนด

(6) กรณีการประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการเนรเทศ การส่งผู้ร้ายข้ามแดน ความร่วมมือระหว่างประเทศเกี่ยวกับกระบวนการยุติธรรมทางอาญา การป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ความร่วมมืออื่นทางศาล หรือกระบวนการยุติธรรมระหว่างประเทศ

(7) การประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐตามพระราชกฤษฎีกานี้ บรรดาที่มีกฎหมายหรือพระราชกฤษฎีกานี้ให้อำนาจในการขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามหน้าที่และอำนาจที่กฎหมายกำหนดไว้ หน่วยงานของรัฐซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมได้รับการยกเว้นเช่นเดียวกัน

แม้ว่าผู้ควบคุมข้อมูลส่วนบุคคลตามที่ระบุไว้ในพระราชกฤษฎีกาข้างต้นจะได้รับการยกเว้นการปฏิบัติตาม PDPA ในหมวด 2 และ 3 แต่เขาก็ยังคงมีหน้าที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด

1.2 นิยามข้อมูลส่วนบุคคล

(1) ข้อมูลส่วนบุคคล (Personal Data)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดนิยามของข้อมูลส่วนบุคคลไว้ตามมาตรา 6 หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตัวอย่างเช่น ชื่อ นามสกุล ชื่อเล่น หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคารของบุคคล ข้อมูลไอพี แอดเดรส (IP address) เป็นต้น

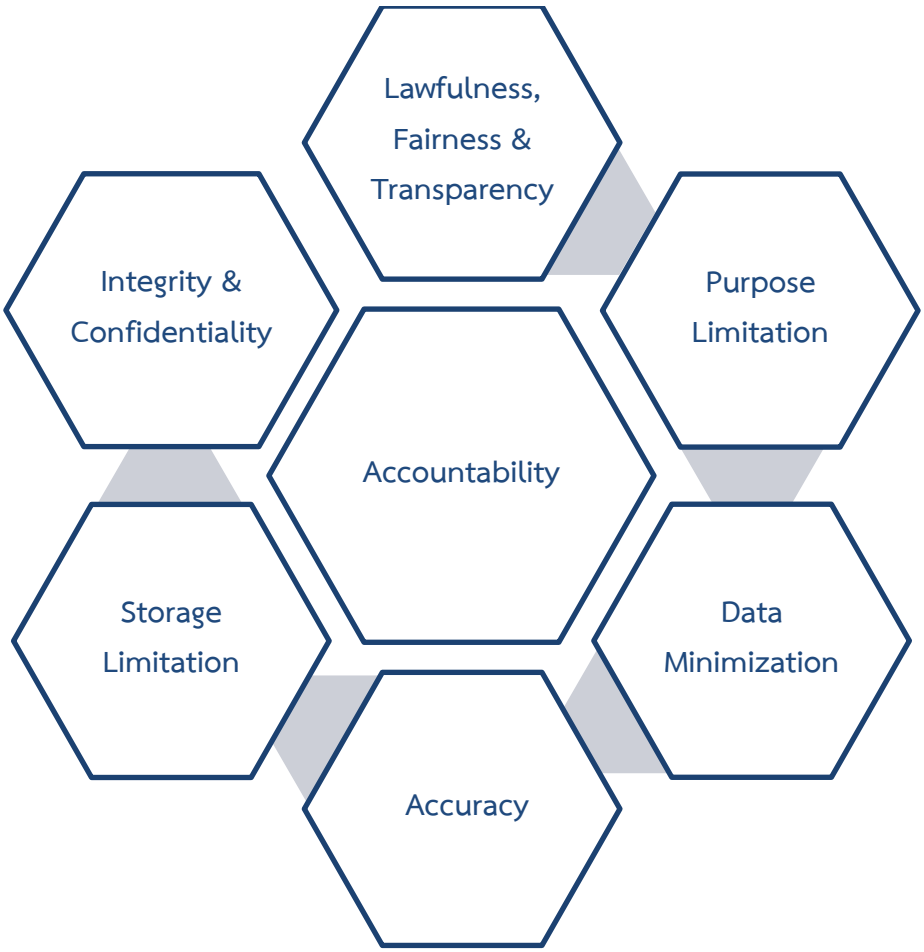
อย่างไรก็ดี ข้อมูลต่อไปนี้ไม่เป็นข้อมูลส่วนบุคคล เช่น ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล อาทิ ชื่อบริษัท ที่อยู่ของบริษัท เลขทะเบียนนิติบุคคลของบริษัท หมายเลขโทรศัพท์ของที่ทำงาน ที่อยู่อีเมล (e-mail address) ของบริษัท เช่น info@company.co.th ข้อมูลนิรนาม (Anonymous Data) ข้อมูลผู้ถึงแก่กรรม เป็นต้น

(2) ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data)

ข้อมูลส่วนบุคคลชนิดพิเศษ (Special categories of personal data) หรือที่ทราบกันดีในนามข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) หมายถึง ข้อมูลส่วนบุคคลตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

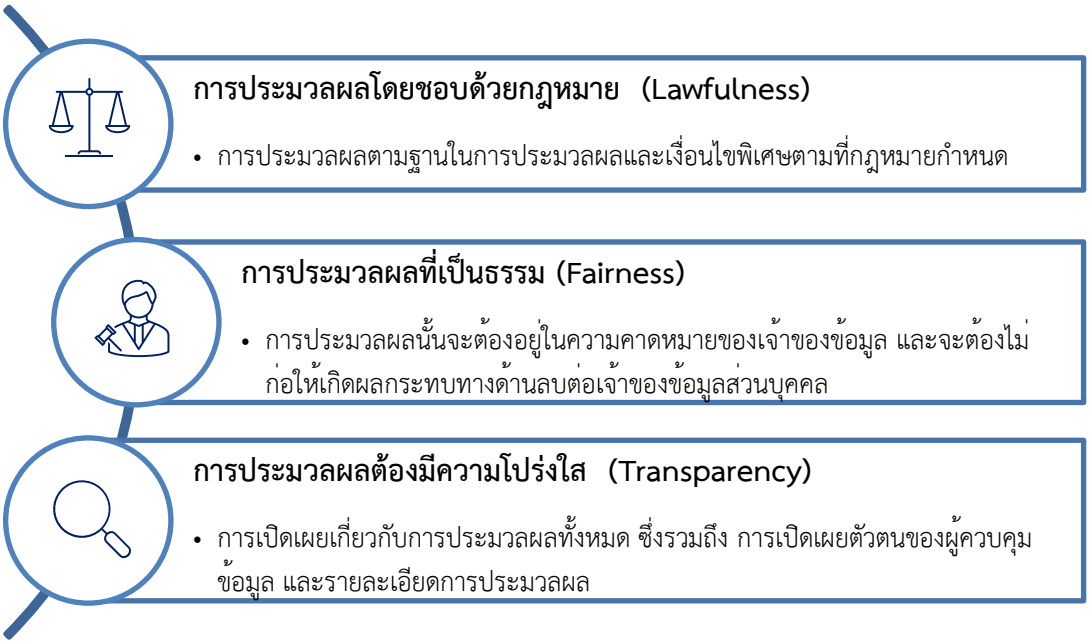
1.3 หลักการในการประมวลผลข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล หรือที่เรียกรวมกันว่าการประมวลผลข้อมูลส่วนบุคคลนั้น มีหลักการ 7 ประการ ดังต่อไปนี้


Lawfulness,
Fairness &
Transparency
Integrity &
Confidentiality
Purpose
Limitation
Accountability
Storage
Limitation
Data
Minimization
Accuracy

1) หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness Fairness and Transparency)

การประมวลผลข้อมูลส่วนบุคคลจะมีขึ้นได้เฉพาะกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นมีเหตุผลความจำเป็นที่สามารถอ้างอิงฐานการประมวลผลทางกฎหมาย (legal basis) ที่กฎหมายรับรองตามมาตรา 24 และมาตรา 26 รวมทั้งจะต้องมีการประกาศและแสดงให้ทราบถึงเหตุผลความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 23 อย่างเปิดเผย และง่ายต่อการทำความเข้าใจเพื่อให้สามารถตัดสินใจต่อการประมวลผลข้อมูลที่อาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้



2) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)

การประมวลผลข้อมูลส่วนบุคคล ตามหลักการจำกัดวัตถุประสงค์ ได้มีการกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 21 กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม โดยการประมวลผลข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่แจ้งไว้ จะไม่สามารถกระทำได้ เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคล ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน หรือมีฐานทางกฎหมายตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล อนุญาตให้ดำเนินการได้

3) หลักการใช้ข้อมูลอย่างจำกัด (Data Minimisation)

การเก็บรวบรวม ใช้ เปิดเผย หรือการประมวลผลข้อมูลส่วนบุคคลนั้น ควรดำเนินการเท่าที่จำเป็นภายใต้วัตถุประสงค์ อันชอบด้วยกฎหมายตามมาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ ควรพิจารณาอย่างรอบคอบ โดยพิจารณาเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นเพียงเท่าที่บรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมนั้น ตัวอย่างเช่น การจัดเก็บสำเนาบัตร

ประชาชน ซึ่งมีข้อมูลศาสนาซึ่งเป็นข้อมูลอ่อนไหวตามมาตรา 26 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องพิจารณาว่าการเก็บข้อมูลศาสนาดังกล่าว มีความจำเป็นต้องเก็บเพื่อบรรลุวัตถุประสงค์ในการดำเนินการกิจกรรมใดหรือไม่ เพราะถ้าหากไม่มีความจำเป็นในการเก็บแล้ว ควรมีมาตรการ เช่น การถมดำ หรือการขีดฆ่าข้อมูลศาสนา เพื่อเป็นการลดภาระหน้าที่ของผู้ควบคุมข้อมูลในการจัดให้มีมาตรการความมั่นคงปลอดภัยที่สูงกว่าข้อมูลส่วนบุคคลทั่วไปในการเก็บข้อมูลส่วนบุคคลอ่อนไหว

4) หลักความถูกต้องของข้อมูล (Accuracy)

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันตามมาตรา 35 โดยผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller จะต้องดำเนินการเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบ หรือแก้ไขโดยไม่ชักช้า และควรมีการจัดช่องทางการติดต่อที่ง่าย สะดวก รวดเร็ว

5) หลักการการจัดเก็บข้อมูลอย่างจำกัด (Storage Limitation)

ข้อมูลส่วนบุคคลจะต้องเก็บในระยะเวลาที่เหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ในการประมวลผลข้อมูล ซึ่งหลักการดังกล่าวปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (3) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ ทั้งนี้ เจ้าของข้อมูลย่อมมีสิทธิขอให้ลบหรือทำลายข้อมูลได้ตามมาตรา 33

6) หลักการธำรงไว้ซึ่งความถูกต้องสมบูรณ์และความลับของข้อมูล (Integrity and Confidentiality)

มาตรการที่จะรักษาความปลอดภัยให้ข้อมูลส่วนบุคคลนั้นจะต้องมีความสมบูรณ์ ไม่ผิดเพี้ยน และจะต้องไม่มีใครแก้ไขข้อมูลหากไม่มีสิทธิ มีการเก็บข้อมูลส่วนบุคคลอย่างเป็นความลับและต้องไม่มีใครเข้าถึงข้อมูลหากไม่มีสิทธิ และความพร้อมใช้งาน ต้องไม่มีใครเข้าครอบครองข้อมูลหากไม่มีสิทธิ โดยเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37(1) และผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา 40(2)

7) หลักความรับผิดชอบของผู้ควบคุมข้อมูล (Accountability)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามหลักการที่กล่าวมาทั้งหกหลักการข้างต้น และดำเนินการตามบทบาทหน้าที่ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบัญญัติไว้ นอกจากนี้ผู้ที่มีอำนาจในการดำเนินกิจการของผู้ควบคุมข้อมูลนั้น มีความรับผิดชอบทางกฎหมายตามมาตรา 81 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือ ในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

1.4 บุคคลที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เจ้าของข้อมูลส่วนบุคคล หมายถึง ผู้มีสิทธิตามกฎหมาย ซึ่งข้อมูลนั้นบ่งชี้ไปถึงบุคคลดังกล่าวไม่ว่าทางตรงหรือทางอ้อม โดยเจ้าของข้อมูลส่วนบุคคลหมายถึงบุคคลธรรมดาเท่านั้นและไม่รวมถึงนิติบุคคล (Juristic Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท สมาคม มูลนิธิ หรือองค์กรอื่นใด ทั้งนี้ เจ้าของข้อมูลส่วนบุคคล สามารถแบ่งประเภทบุคคลได้ดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะ

(1) บุคคลที่มีอายุตั้งแต่ 20 ปีบริบูรณ์ขึ้นไป

(2) ผู้ที่สมรสตามกฎหมายตั้งแต่อายุ 17 ปีบริบูรณ์ขึ้นไป

(3) ผู้ที่สมรสก่อนอายุ 17 ปี โดยศาลอนุญาตให้ทำการสมรส

(4) ผู้เยาว์ซึ่งผู้แทนโดยชอบธรรมให้ความยินยอมในการประกอบธุรกิจทางการค้าหรือธุรกิจอื่น หรือในการทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน ในความเกี่ยวพันกับการประกอบธุรกิจหรือ การจ้างแรงงานข้างต้นให้ผู้เยาว์มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว

ทั้งนี้ ในการให้ความยินยอมใด ๆ เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะสามารถให้ความยินยอมได้ด้วยตนเอง

2) เจ้าของข้อมูลส่วนบุคคลที่เป็น “ผู้เยาว์”

หมายถึง บุคคลที่อายุต่ำกว่า 20 ปีบริบูรณ์ และไม่ใช่ผู้บรรลุนิติภาวะตามข้อ 1) ทั้งนี้ ในการให้ความยินยอมใด ๆ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 20

3) เจ้าของข้อมูลส่วนบุคคลที่เป็น “คนเสมือนไร้ความสามารถ”

หมายถึง บุคคลที่ศาลสั่งให้เป็นคนเสมือนไร้ความสามารถเนื่องจากมีกายพิการหรือมีจิตฟั่นเฟือนไม่สมประกอบ หรือประพฤติสุรุ่ยสุร่ายเสเพลเป็นอาจิณ หรือติดสุรายาเมา หรือมีเหตุอื่นใดทำนองเดียวกันนั้น จนไม่สามารถจะจัดทำการงานโดยตนเองได้ หรือจัดกิจการไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือครอบครัวทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถนั้นก่อน

4) เจ้าของข้อมูลส่วนบุคคลที่เป็น “คนไร้ความสามารถ”

หมายถึง บุคคลที่ศาลสั่งให้เป็นคนไร้ความสามารถ เช่น เป็นบุคคลวิกลจริต ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถนั้นก่อน

2. ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller

ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นผู้ประกอบการที่ทำธุรกิจในนามบุคคลธรรมดา หรือทำในรูปแบบนิติบุคคล ไม่ว่าจะประกอบกิจการเป็นบริษัทจำกัด บริษัทมหาชนจำกัด หรือนิติบุคคลในรูปแบบอื่นที่ไม่ใช่บริษัท และไม่ได้จำกัดแต่เฉพาะในภาคเอกชนเท่านั้น แต่ยังรวมถึงหน่วยงานของรัฐที่อำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ย่อมมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล ดังต่อไปนี้

1) เก็บรวบรวม ใช้ เปิดเผย ให้เป็นไปตามกฎหมาย

การเก็บรวบรวม ใช้ เปิดเผย ต้องมีฐานทางกฎหมายรองรับ ดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ และต้องดำเนินการเก็บรวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้น ซึ่งเกี่ยวข้องกับหน้าที่ในการจัดเตรียมเอกสารต่าง ๆ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมั่นใจว่าหากยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลเข้าไปเก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอย่างไร

2) ดำเนินการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

กรณีมีคำร้องขอของเจ้าของข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคล ปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องระบุเหตุผลในบันทึกรายการตามมาตรา 39 ตัวอย่างเช่น พนักงานของบริษัทขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคล แต่การเข้าถึงดังกล่าวนั้นไปกระทบสิทธิของบุคคลอื่น เช่นนี้บริษัทมีสิทธิในการปฏิเสธได้ และต้องมีการบันทึกเหตุแห่งการปฏิเสธไว้

3) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเป็นไปตามมาตรฐานขั้นต่ำ ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของเจ้าของข้อมูลส่วนบุคคล ว่าในกิจกรรมนั้น ๆ ว่าฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อคกุญแจหรือไม่

4) จัดให้มีมาตรการป้องการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ

ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น มีการโอนข้อมูลส่วนบุคคลให้ผู้ประมวลผล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ถูกต้องตามกฎหมาย

5) จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

6) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ล่าช้า

7) แต่งตั้งตัวแทนในราชอาณาจักร

หากผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกประเทศไทย ผู้ควบคุมส่วนบุคคลต้องแต่งตั้งตัวแทนของตนในประเทศไทย โดยต้องแต่งตั้งเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในประเทศไทยและได้รับมอบอำนาจให้กระทำแทนโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของผู้ควบคุมข้อมูล

8) หน้าที่ในการจัดทำบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities : RoPA)

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องบันทึกรายการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

9) จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

10) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีลักษณะเข้าหลักเกณฑ์ที่กฎหมายกำหนดตามมาตรา 41 ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่ง หรือ ในนามหรือภายใต้คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

1) ประมวลผลข้อมูลส่วนบุคคลภายใต้คำสั่งผู้ควบคุมข้อมูล

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุ การละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของเจ้าของข้อมูลส่วนบุคคลว่าในกิจกรรมนั้น ๆ ว่าฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อคกุญแจหรือไม่

3) จัดทำบันทึกรายการประมวลผล ข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรม การประกาศกำหนด

4) ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อสังเกต : พนักงานในหน่วยงาน องค์กร หรือสถาบัน ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) พนักงานของนิติบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่กระทำตามคำสั่งหรือในนามของนิติบุคคลนั้นไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

ตามมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้

(1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

โดยประกาศคณะกรรมการกำหนดให้หน่วยงานรัฐที่ต้องมี DPO เช่น สำนักงานคณะกรรมการข้าราชการพลเรือน กรมบัญชีกลาง กรมการกงสุล กรมการท่องเที่ยว กรมการขนส่งทางบก กรมพัฒนาธุรกิจการค้า กรมการปกครอง กรมการจัดหางาน กรมการแพทย์ กรุงเทพมหานคร การทางพิเศษแห่งประเทศไทย ธนาคารกรุงไทย ธนาคารออมสิน มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น[1]

(2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

โดยประกาศคณะกรรมการได้มีการวางหลักเกณฑ์ที่สำคัญ กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะครบทั้ง 3 องค์ประกอบ จะต้องมีการแต่งตั้ง DPO โดยองค์ประกอบทั้งสามประการ มีดังนี้[2]

องค์ประกอบประการแรก การดำเนินกิจกรรมในการประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) โดยกิจกรรมหลัก หมายถึง การดำเนินการที่จำเป็นและสำคัญต่อเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล แต่ไม่รวมถึงกิจกรรมเสริมที่เป็นงานสนับสนุนในการดำเนินงานซึ่งไม่ใช่การดำเนินงานที่จำเป็นและสำคัญเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ในประกาศฯ ได้ยกตัวอย่างว่า การประมวลผลข้อมูลส่วนบุคคลของลูกค้าเพื่อการให้บริการแก่ลูกค้าและบันทึกการรับบริการของลูกค้าเป็นการดำเนินการที่จำเป็นและสำคัญต่อการให้บริการรับจ้างขนส่งสินค้า หรือการประมวลผลข้อมูลส่วนบุคคลจากกล้องวงจรปิดเป็นการดำเนินการที่จำเป็นและสำคัญต่อการรับจ้างรักษาความปลอดภัย แต่ไม่รวมถึงงานสนับสนุนด้านบุคลากรและเทคโนโลยี

---

[1] สามารถดูรายชื่อหน่วยงานรัฐทั้งหมดตามประกาศได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf

[2] สามารถดูรายละเอียดของประกาศฉบับนี้ได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf

สารสนเทศซึ่งเป็นเพียงงานสนับสนุนสำหรับการให้บริการรับจ้างขนส่งสินค้าหรือการรับจ้างรักษาความปลอดภัยให้กับสถานที่ต่าง ๆ

องค์ประกอบประการที่สอง การดำเนินกิจกรรมนั้นมีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ หมายถึง การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลักที่มีการเฝ้าติดตาม (track) เฝ้าสังเกต (monitor) วิเคราะห์ หรือทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคลอย่างเป็นระบบ (profile) และเกิดขึ้นเป็นประจำหรือปกติธุระ (regular)

โดยในกรณีดังต่อไปนี้ จะถือเป็นกรณีที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ

- การประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์ หรือบัตรอื่นใดที่มีลักษณะเดียวกันซึ่งผู้ให้บริการสามารถตรวจสอบรายละเอียดข้อมูลการใช้งานบัตรได้

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการซึ่งเกิดเป็นปกติธุระหรือประจำที่มีการตรวจสอบสถานะ ประวัติ คุณสมบัติก่อนเข้าทำสัญญาหรือให้บริการเพื่อประเมินความเสี่ยงด้านต่าง ๆ เช่น การให้คะแนนเครดิต การพิจารณาเบี้ยประกันภัย การป้องกันการฉ้อฉล เป็นต้น

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาติดตามพฤติกรรม (behavioral advertising)

- การประมวลผลข้อมูลส่วนบุคคลของของลูกค้าหรือผู้รับบริการโดยผู้ให้บริการระบบเครือข่ายคอมพิวเตอร์หรือผู้ประกอบกิจการโทรคมนาคม

- การประมวลผลข้อมูลส่วนบุคคลเพื่อการเฝ้าระวังและรักษาความปลอดภัยตามสถานที่ต่าง ๆ

- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

และองค์ประกอบประการสุดท้าย กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale) โดยจะพิจารณาจากปัจจัย ดังต่อไปนี้

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือสัดส่วนเจ้าของข้อมูลที่ประมวลผล เมื่อเทียบกับจำนวนเจ้าของข้อมูลทั้งหมดที่อาจเป็นไปได้

- ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่ประมวลผล

- ระยะเวลาหรือความคงอยู่ของการประมวลผลเพื่อประโยชน์ในการดำเนินกิจกรรมหลัก

- ขอบเขตการใช้ข้อมูลส่วนบุคคลขององค์กร หรือตามขนาดพื้นที่หรือจำนวนประเทศที่เกี่ยวข้องกับการประมวลผล

โดยในกรณีดังต่อไปนี้ จะถือเป็น กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale)

- การประมวลผลข้อมูลส่วนบุคคลจำนวนตั้งแต่ 100,000 รายขึ้นไป

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม ผ่านโปรแกรมค้นหาหรือสื่อสังคมออนไลน์

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานโดยปกติของบริษัทตามกฎหมายว่าด้วยประกันชีวิตและกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้รับใบอนุญาตประกอบธุรกิจโทรคมนาคมแบบที่สามตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม

- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ดังนั้น หากผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายใดที่การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) ที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ และมีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามที่คณะกรรมการประกาศกำหนด ตามมาตรา 29 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานที่ทำการแต่ละแห่งของผู้ควบคุม ข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าว ต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย และในส่วนของการกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ต้องเป็นไปตามที่คณะกรรมการประกาศกำหนด โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

คุณสมบัติและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นจะเป็นพนักงาน ผู้รับจ้างของผู้ควบคุมข้อมูล หรือ ผู้ประมวลผลข้อมูล โดยอาจจะเป็นคนเดียวหรือคณะทำงานก็ได้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลส่วนบุคคลและรายละเอียดการประมวลผลภายในองค์กรได้รับการสนับสนุนที่เพียงพอ ด้านอุปกรณ์ เครื่องมือ งบประมาณ และอำนวยความสะดวกในการเข้าถึง ได้รับความคุ้มครองจากการถูกเลิกจ้างด้วยเหตุที่ปฏิบัติหน้าที่ตามพระราชบัญญัติ รวมถึงในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ต้องสามารถรายงานถึงผู้บริหารสูงสุดขององค์กรและควรได้โดยตรงได้

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีดังนี้

1) ให้คำแนะนำ

ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

2) ตรวจสอบการดำเนินการ

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3) ประสานงานและให้ความร่วมมือกับสำนักงาน

ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

4) รักษาความลับของข้อมูล

รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

1.5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไว้ในหมวด 2 ของพระราชบัญญัติ ซึ่งได้กำหนดหลักเกณฑ์ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ตั้งแต่กระบวนการเก็บรวบรวม เช่น การกำหนดวัตถุประสงค์ ฐานกฎหมายที่อ้างอิงในการประมวลผลข้อมูล แหล่งที่มาของข้อมูล การแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล เป็นต้น ตลอดจนหลักเกณฑ์ในการใช้และการเปิดเผยข้อมูลส่วนบุคคล เช่น การเปิดเผยข้อมูลให้แก่บุคคลภายนอก การโอนข้อมูลไปต่างประเทศ เป็นต้น

การดำเนินการประมวลผลข้อมูลส่วนบุคคล สิ่งที่สำคัญและมีความจำเป็นสำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องคำนึงเป็นประการแรกในการเริ่มต้นกระบวนการประมวลผลข้อมูลส่วนบุคคล คือ การพิจารณาเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ตามหลักใช้ข้อมูลอย่างจำกัด (Data Minimisation) สิ่งสำคัญคือการกำหนดวัตถุประสงค์ เปรียบเสมือนกระดุมเม็ดแรกในการประมวลผลข้อมูลส่วนบุคคล การได้มาซึ่งวัตถุประสงค์ที่ชัดเจน จะช่วยให้สามารถระบุได้ว่าเพื่อบรรลุวัตถุประสงค์ดังกล่าว ข้อมูลส่วนบุคคลที่จำเป็นต้องเก็บรวบรวมแท้จริงนั้นมีข้อมูลประเภทใดบ้าง เป็นข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลส่วนบุคคลประเภทอ่อนไหว เพื่อนำไปสู่กระบวนการต่อไปหรือกระดุม

เม็ดถัดไป ในการกำหนดฐานกฎหมาย ซึ่งแน่นอนว่าฐานกฎหมายของข้อมูลส่วนบุคคลแต่ละประเภทกฎหมายกำหนดฐานไว้แตกต่างกัน โดยเฉพาะข้อมูลส่วนบุคคลประเภทอ่อนไหว ซึ่งต้องใช้ความระมัดระวังในการประมวลผลข้อมูลเป็นพิเศษ ทั้งนี้เพื่อความเข้าใจมากยิ่งขึ้น จึงขอยกเรื่องฐานทางกฎหมายสำหรับข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลประเภทอ่อนไหว ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาทำความเข้าใจกัน ดังนี้

ฐานทางกฎหมาย (Lawful Basis)

1) ฐานทางกฎหมายในการประมวลข้อมูลส่วนบุคคล ซึ่งมาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดไว้ 7 ฐาน ดังต่อไปนี้

- **ฐานความยินยอม (Consent)**

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจาก เจ้าของข้อมูลส่วนบุคคล ก่อนหรือในขณะการเก็บรวบรวมนั้น เว้นแต่มีฐานทางกฎหมายอื่นอนุญาตให้เก็บรวบรวมได้ ทั้งนี้ การขอความยินยอมจะต้องมีรูปแบบตามที่กำหนดไว้ในมาตรา 19 กล่าวคือ

(1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล

(2) การขอความยินยอมต้องทำโดยชัดแจ้ง แยกส่วนจากข้อความอื่นอย่างชัดเจน

(3) แจ้งวัตถุประสงค์อย่างชัดเจน

(4) มีแบบ และข้อความที่ เข้าถึงได้ง่าย และเข้าใจได้

(5) ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงทำให้เข้าใจผิดในวัตถุประสงค์

(6) การให้ความยินยอมต้องมีความอิสระ และต้องไม่เป็นส่วนหนึ่งของสัญญาหรือบริการ

(7) ต้องถอดถอนง่ายเช่นเดียวกับตอนให้ความยินยอม และจะถอนความยินยอมเมื่อใดก็ได้

(8) หากการถอนความยินยอมมีผลกระทบในเรื่องใด ต้องแจ้งให้เจ้าของข้อมูลทราบ

กรณีเจ้าของข้อมูลส่วนบุคคล เป็นบุคคลหย่อนความสามารถ อันได้แก่ ผู้เยาว์ ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมาย คนเสมือนไร้ความสามารถ และคนไร้ความสามารถ การขอความยินยอมกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหลักเกณฑ์ในการขอความยินยอมเพิ่มเติม ปรากฏตามมาตรา 20 ดังนี้

(1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง

(2) ผู้เยาว์อายุ 10 ปี แต่ยังไม่ถึง 20 ปีบริบูรณ์ อาจให้ความยินยอมโดยลำพังหรือจาก ผู้ใช้อำนาจ ปกครองผู้เยาว์

(3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์

(4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

รวมถึงการถอนความยินยอม การแจ้งให้ทราบ การใช้สิทธิ การร้องเรียน และอื่น ๆ ตามพระราชบัญญัติ ให้กระทำโดยผู้มีอำนาจตาม (1) - (4) ด้วย

- **ฐานปฏิบัติตามสัญญา (Contract)**

ฐานสัญญาถือเป็นฐานที่จำเป็นเพื่อการปฏิบัติตามสัญญาและใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา เช่น การขอสินเชื่อเพื่อเปิดบัญชีเงินฝาก การให้สินเชื่อ การทวงถามหนี้สินที่ต้องประมวลข้อมูลการเงิน โดยฐานปฏิบัติตามสัญญา จำเป็นเพื่อปฏิบัติตามสัญญาโดยตรงทั้งก่อนและเข้าทำสัญญาทางการค้าแม้ไม่ได้ระบุเป็นเงื่อนไขในสัญญา เฉพาะข้อมูลส่วนบุคคลทั่วไปของเจ้าของข้อมูลคู่สัญญาเท่านั้นเมื่อเข้าฐานปฏิบัติตามสัญญาก็ไม่ต้องขอความยินยอมเพิ่มเติม และเมื่อไม่ใช่ฐานความยินยอม จึงไม่อาจถอนความยินยอมได้

- **ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)**

ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกรณีที่มีกฎหมายกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการในการประมวลผลข้อมูล

- **ฐานผลประโยชน์สาธารณะ อำนาจรัฐ (Public Task)**

ผู้ประมวลผลข้อมูลตามฐานนี้มักเป็นเจ้าหน้าที่ หรือหน่วยงานของรัฐที่มีหน้าที่ในการปฏิบัติตามภารกิจที่มีกฎหมายกำหนดไว้ รวมถึงหน่วยงานเอกชนหากการประมวลผลข้อมูลนั้นมีความจำเป็นหรือหน้าที่ต้องปฏิบัติตามกฎหมายหรือเป็นไปเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย

- **ฐานผลประโยชน์อันชอบธรรมด้วยกฎหมาย (Legitimate Interest)**

ผู้ประมวลผลข้อมูลจะต้องใช้ฐานนี้ในกรณีที่จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล และเป็นไปอย่างสมเหตุสมผล เช่น การตรวจสอบอาชญากรรมและการฉ้อโกง อันส่งผลต่อหน่วยงานหรือเป็นการช่วยเหลือเจ้าหน้าที่รัฐตามกฎหมาย ในฐานนี้ตามกฎหมายมาตรา 24 มีหลัก 3 ข้อ

(1) จะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล

(2) มีความเสี่ยงต่อการกระทบสิทธิเสรีภาพของเจ้าของข้อมูลในระดับต่ำ

(3) มีความชอบธรรม

- **ฐานระงับอันตรายต่อ ร่างกาย สุขภาพ หรือชีวิต (Vital Interest)**

ฐานระงับอันตรายต่อร่างกายสุขภาพและชีวิต กรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลส่วนบุคคล ในขณะ หรือสถานการณ์ที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เช่น เจ้าของข้อมูลส่วนบุคคลเกิดอุบัติเหตุ หมดสติ จะต้องเก็บข้อมูลเพื่อผดุงชีพเบื้องต้น เป็นต้น

- **ฐานการจัดทำเอกสารประวัติศาสตร์-วิจัย-สถิติ และจดหมายเหตุ (Historical Document, Research, or Statistics)**

ฐานจดหมายเหตุ วิจัย สถิติ ควรเป็นไปตามมาตรฐานการวิจัย เป็นการเก็บรวบรวม จัดเก็บข้อมูลเพื่อการจัดทำเอกสารทางประวัติศาสตร์ หรืองานวิจัย หรืองานสถิติ ซึ่งจะต้องมีการระบุชัดเจน

2) ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลประเภทอ่อนไหว ซึ่งมาตรา 26 กำหนดไว้มี 6 ฐาน ดังต่อไปนี้

- **ฐานความยินยอมโดยชัดแจ้ง**

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่มีฐานทางกฎหมายอื่นอนุญาตให้เก็บรวบรวมได้ ทั้งนี้ รูปแบบการขอความยินยอม และหลักเกณฑ์การขอความยินยอมสำหรับบุคคลหย่อนความสามารถ ให้ดำเนินการตามที่กำหนดไว้ใน มาตรา 19 และ 20 เช่นเดียวกับฐานความยินยอม สำหรับข้อมูลส่วนบุคคลทั่วไป

- **ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล**

เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ฐานระงับอันตรายต่อร่างกายสุขภาพและชีวิตกรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อน (sensitive data) เช่น กรุ๊ปเลือด ข้อมูลสุขภาพ สามารถใช้ได้กรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เช่น เจ้าของข้อมูลส่วนบุคคลเกิดอุบัติเหตุ เป็นต้น

- **ฐานการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสม**

การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร โดยต้องไม่เปิดเผยไปสู่บุคคลภายนอก

- **ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล**

  กรณีที่เจ้าของข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลประเภทอ่อนไหวของตนเองต่อพื้นที่สาธารณะด้วยความสมัครใจของตนเอง เช่น กรณีเจ้าของข้อมูลส่วนบุคคลเปิดเผยข้อมูลพฤติกรรมทางเพศของตน ว่ามีรสนิยมทางเพศ เป็น LGBTQ+ บนช่องทางโซเชียลมีเดียของตน ด้วยความยินยอมโดยชัดแจ้ง เช่นนี้อาจพิจารณาใช้ฐานดังกล่าวได้

- **ฐานความจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย**

  การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

- **ฐานความจำเป็นต้องปฏิบัติตามกฎหมาย**

  กรณีมีความจำเป็นต้องปฏิบัติตามกฎหมาย ซึ่งเกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์การประเมินความสามารถในการทำงานของเจ้าของข้อมูลส่วนบุคคล การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการใช้บริการด้านสังคมสงเคราะห์ ประโยชน์สาธารณะด้านสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นที่สำคัญ

การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 บัญญัติห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

ทั้งนี้ ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนการประมวลผล ตามมาตรา 21 และการแจ้งรายละเอียดในการเก็บ

รวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามมาตรา 25 วรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

(1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิเสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามมาตรา 25 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 30 วันนับแต่วันที่เก็บรวบรวมข้อมูลส่วนบุคคลนั้น เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

การใช้ หรือการเปิดเผยข้อมูล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 บัญญัติห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

ทั้งนี้ บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามมาตรา 27 จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น อย่างไรก็ตามในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 27 วรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39

การส่งหรือโอนข้อมูลไปต่างประเทศ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 28 บัญญัติในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือ

องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

(6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

บทบัญญัติมาตรา 29 กำหนดในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองดังกล่าวให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28

1.6 ความรับผิดและบทกำหนดโทษ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

<u>ความรับผิดทางแพ่ง</u>

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดความรับผิดทางแพ่งไว้ตามมาตรา 77 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใดเกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วน

บุคคล ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล จะต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น ซึ่งค่าสินไหมทดแทนดังกล่าวรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นแล้ว

ทั้งนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคล บัญญัติให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น

<u>โทษอาญา</u>

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดบทกำหนดโทษในส่วนของโทษอาญาไว้ในกรณีต่าง ๆ ดังต่อไปนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) โดยมิชอบหรือนอกเหนือวัตถุประสงค์ หรือส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) ไปยังต่างประเทศ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ ทั้งนี้ หากการฝ่าฝืนของผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวมีเจตนาพิเศษเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จะต้องระวางโทษจำคุกไม่เกิน 1 ปีปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ความผิดในมาตรานี้เป็นความผิดอันยอมความได้ มาตรา 79

2) ผู้ใดซึ่งล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้แล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 500,000 บาท หรือ ทั้งจำทั้งปรับ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 80

โดยมีข้อยกเว้น สำหรับบทลงโทษนี้ มิให้นำมาบังคับใช้แก่การเปิดเผย ในกรณีดังนี้

1) เปิดเผยตามหน้าที่

2) เปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือพิจารณาคดี

3) เปิดเผยแก่หน่วยงานรัฐในประเทศ หรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

4) ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

5) การเปิดเผยเกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

3) กรรมการหรือผู้จัดการหรือบุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคล หากมีการสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลกระทำความผิดต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย

<u>โทษทางปกครอง</u>

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบัญญัติบทกำหนดโทษ ส่วนของโทษทางปกครองในหมวดที่ 7 ตามมาตรา 82 ถึง มาตรา 90 โดยระวางปรับทางปกครองสูงสุดไม่เกิน 5,000,000 บาท แล้วแต่กรณี

การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญจะพิจารณาถึง

- ความร้ายแรงแห่งพฤติกรรมที่กระทำ
- ขนาดกิจการของผู้ควบคุมข้อมูล หรือผู้ประมวลผล
- พฤติการณ์ต่าง ๆ

ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการกำหนด มาตรา 90 วรรค 2

โดยตามระดับของความร้ายแรงของการกระทำความผิด บทลงโทษทางปกครองจะพิจารณาตามระดับความร้ายแรงของการกระทำความผิด ดังนี้

<u>กรณีไม่ร้ายแรง</u>

คณะกรรมการผู้เชี่ยวชาญจะออกคำสั่ง

1) ตักเตือน สั่งให้ปฏิบัติ แก้ไขให้ถูกต้อง หยุด ระงับ ละเว้น งดเว้นการกระทำ ภายในระยะเวลาที่กำหนด

2) สั่งห้ามให้ปฏิบัติ หรือให้ปฏิบัติเพื่อระงับความเสียหาย ภายในระยะเวลาที่กำหนด

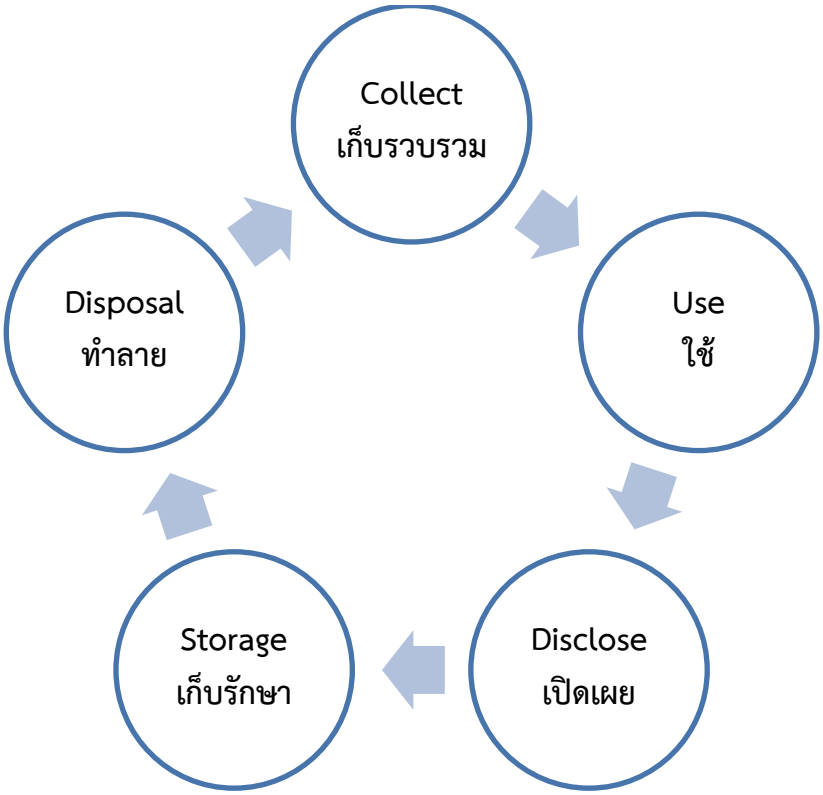
3) สั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ภายในระยะเวลาที่กำหนด

<u>กรณีร้ายแรง หรือคำสั่งให้แก้ไข หรือตักเตือนไม่เป็นผล</u>

คณะกรรมการผู้เชี่ยวชาญจะออกคำสั่งลงโทษปรับทางปกครองโดยคำนึงถึงความร้ายแรง พฤติการณ์อื่น และอาจมีคำสั่งให้ตักเตือน สั่งให้ปฏิบัติ แก้ไขให้ถูกต้อง หยุด ระงับ ละเว้น งดเว้นการกระทำ สั่งให้ปฏิบัติ หรือห้ามปฏิบัติเพื่อระงับความเสียหาย สั่งจำกัดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วยก็ได้ภายในระยะเวลาที่กำหนด

บทที่ 2 แนวทางการดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับสำนักงานสอบบัญชี

กิจกรรมการประมวลผลข้อมูลส่วนบุคคลของสำนักงานสอบบัญชี ต่างมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งแต่ละสำนักงานต่างมีข้อมูลส่วนบุคคลไหลเวียนภายในเป็น “วงจรชีวิตของข้อมูล” (data life cycle) โดยหากสำนักงานสอบบัญชีเข้าใจแนวคิดเรื่องวงจรชีวิตของข้อมูล ก็จะช่วยให้สามารถเห็นภาพการไหลเวียนของข้อมูล และเห็นช่องว่างในกระบวนการการดำเนินการของสำนักงานของตนว่ามีมาตรการเก็บรวบรวม เก็บรักษา ใช้ เปิดเผยหรือโอน และทำลายข้อมูลส่วนบุคคลเหมาะสมหรือไม่ ทั้งนี้ วงจรชีวิตของข้อมูล มีองค์ประกอบ และแนวทางในการพิจารณาในแต่ละขั้นตอน ดังนี้



การเก็บรวบรวมข้อมูล (Collection)

- การเก็บรวบรวมข้อมูล ควรพิจารณาเก็บเท่าที่จำเป็นและไม่เกินวัตถุประสงค์ที่เก็บ (ตามหลัก Data Minimization)
- ผู้ควบคุมข้อมูลจะต้องระบุและแจ้งวัตถุประสงค์ในการเก็บข้อมูล โดยกำหนดวัตถุประสงค์และฐานทางกฎหมาย (lawful basis)

- แจ้งวัตถุประสงค์การเก็บข้อมูลผ่าน “ประกาศความเป็นส่วนตัว” (Privacy Notice) โดยให้มีรายละเอียดอย่างน้อยตามที่กำหนดไว้ในมาตรา 23

การใช้หรือเปิดเผยข้อมูล (Use or Disclosure)

- พิจารณาว่าองค์กรมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลภายนอกประเภทใดบ้าง และการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว มีฐานทางกฎหมายรองรับให้สามารถเปิดเผยได้หรือไม่
- หากเปิดเผยบุคคลภายนอก พิจารณาจัดทำสัญญาประมวลผลข้อมูลหรือเปิดเผยข้อมูลกับบุคคลภายนอกที่ได้รับข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินการ และความรับผิดที่อาจเกิดขึ้น
- แจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อมีการใช้หรือโอนข้อมูลเกินกว่าวัตถุประสงค์ที่แจ้งไว้หรือที่ขอความยินยอมตอนเก็บข้อมูล
- เตรียมช่องทางให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

การเก็บรักษา (Storage)

- มีมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสม และกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล
- กำหนดสิทธิของพนักงานให้เข้าถึงข้อมูลภายในบริษัทเท่าที่จำเป็น
- เตรียมช่องทางให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกับข้อมูลของตนเอง
- เตรียมช่องทางแจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อเกิดข้อมูลรั่วไหล

การทำลาย (Disposal)

- ทำลายเมื่อไม่ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้หรือเมื่อครบกำหนดเวลา
- ทำลายด้วยวิธีการที่ไม่เกิดโอกาสให้ข้อมูลรั่วไหลและไม่สามารถระบุตัวตนได้อีก

กิจกรรมการประมวลข้อมูลของสำนักงานสอบบัญชี

สำนักงานสอบบัญชี เป็นธุรกิจที่ประกอบกิจการให้บริการด้านสอบบัญชี ตามพระราชบัญญัติการบัญชี ซึ่งมีตัวอย่างกิจกรรมหลักที่เกิดขึ้นในการประกอบกิจการ ตามวงจรชีวิตของข้อมูล ดังต่อไปนี้

<table>
<tr><th rowspan="2">กิจกรรม</th><th colspan="4">วงจรชีวิตข้อมูล (Data life cycle)</th></tr>
<tr><th>เก็บรวบรวม</th><th>ใช้ / เปิดเผย</th><th>เก็บรักษา</th><th>ทำลาย</th></tr>
<tr><td>1) การทำความเข้าใจองค์กรของผู้ว่าจ้าง เพื่อประเมินความเสี่ยงในการรับงาน</td><td>ข้อมูลส่วนบุคคลของผู้กรรมการ หุ้นส่วน ผู้บริหาร ผู้ประสานงานของผู้ว่าจ้าง และข้อมูลส่วนบุคคลที่ใช้เป็นหลักฐานในการปฏิบัติงานตรวจสอบ</td><td>เพื่อประเมินความเสี่ยงก่อนรับงานสอบบัญชี
• หน่วยงานที่มีอำนาจตามที่กฎหมายกำหนด
• ที่ปรึกษาหรือผู้เชี่ยวชาญภายนอก</td><td rowspan="3">• การเก็บรักษาข้อมูลส่วนบุคคลที่เป็นเอกสาร และไฟล์อิเล็กทรอนิกส์
• การเก็บรักษาข้อมูลส่วนบุคคลที่ได้รับผ่านช่องทางการสื่อสารส่วนบุคคล
• ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล</td><td rowspan="3">การดำเนินการทำลายข้อมูลส่วนบุคคล เมื่อหมดความจำเป็นในการใช้ข้อมูล หรือเสร็จสิ้นการให้บริการสอบบัญชี หรือบริการอื่นที่เกี่ยวข้อง หรือพ้นกำหนดระยะเวลาในการเก็บรักษาข้อมูล</td></tr>
<tr><td>2) การรับงาน และการปฏิบัติงานสอบบัญชี</td><td>ข้อมูลส่วนบุคคลของกรรมการ หุ้นส่วน ผู้มีอำนาจลงนาม ผู้สอบบัญชี ผู้ประสานงาน และข้อมูลส่วนบุคคลที่ใช้เป็นหลักฐานในการปฏิบัติงานตรวจสอบ</td><td>เพื่อปฏิบัติงานสอบบัญชี
• ไม่มีการเปิดเผย</td></tr>
<tr><td>3) การจ้างบุคคลภายนอกเพื่อการปฏิบัติงานสอบบัญชี</td><td>ข้อมูลส่วนบุคคลของผู้เชี่ยวชาญ หรือผู้ช่วยผู้สอบบัญชีที่ว่าจ้างและข้อมูลส่วนบุคคลที่ใช้เป็นหลักฐานในการปฏิบัติงานตรวจสอบ</td><td>เพื่อจัดทำเงินเดือน การยื่นแบบแสดงรายการภาษี และรายการภาษีที่เกี่ยวข้อง
• หน่วยงานที่มีอำนาจตามที่กฎหมายกำหนด</td></tr>
</table>

1. การทำความเข้าใจองค์กรของผู้ว่าจ้าง เพื่อประเมินความเสี่ยงในการรับงาน

ก่อนที่จะรับทำงานสำนักงานสอบบัญชีต้องมีการประเมินความเสี่ยงที่เกิดจากการรับเป็น ผู้สอบบัญชี โดยตรวจสอบประวัติของกรรมการ หุ้นส่วน และผู้บริหาร เป็นต้น

สิ่งที่เจ้าของสำนักงานสอบบัญชีควรระวังหรือพิจารณา ได้แก่

(1) การเก็บรวบรวมข้อมูล (Collection)

กิจกรรมนี้มีประเภทของ ข้อมูลส่วนบุคคลด้านอื่นๆ ที่เกี่ยวข้องกับการพิจารณาเพื่อรับงานสอบบัญชี เช่น

- ชื่อ นามสกุล ตำแหน่ง กรรมการ หุ้นส่วน ผู้บริหาร

- ประวัติการทำงาน กรรมการ หุ้นส่วน ผู้บริหาร
- ชื่อ นามสกุล หมายเลขโทรศัพท์และอีเมลของผู้ประสานงาน
- ข้อมูลการถือหุ้นของ กรรมการ หุ้นส่วน ผู้บริหาร
- ข้อมูลส่วนบุคคลด้านอื่นๆ ที่เกี่ยวข้องกับการพิจารณาเพื่อรับงานสอบบัญชี

แหล่งที่มาของข้อมูลส่วนบุคคลเพื่อใช้ในการประเมินความเสี่ยงก่อนที่จะรับงานสอบบัญชีมาจาก

- บริษัทผู้ว่าจ้างสอบบัญชี ผู้ประสานงาน
- แหล่งอื่น เช่น อินเตอร์เน็ต หนังสือพิมพ์ ตลาดหลักทรัพย์แห่งประเทศไทย เป็นต้น

สำนักงานสอบบัญชีควรต้องดำเนินการ

- ในการได้รับข้อมูลจากแหล่งอื่น และมีการเก็บเป็นเอกสารควรมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ โดยแจ้งภายใน 30 วัน หลังจากที่ได้ตรวจสอบและรับข้อมูล ทั้งนี้ อาจพิจารณาให้บริษัทผู้ว่าจ้างสอบบัญชีดำเนินการแจ้งรายละเอียดการเปิดเผยข้อมูลส่วนบุคคลแก่สำนักงานสอบบัญชีให้เจ้าของข้อมูลทราบ
- ในงานการทำความเข้าใจองค์กรของผู้ว่าจ้างเพื่อประเมินความเสี่ยงก่อนรับงาน ข้อมูลส่วนบุคคลที่สำนักงานสอบบัญชีได้รับ เก็บรวบรวม และเปิดเผยข้อมูล เป็นการใช้ฐานการปฏิบัติตามสัญญาในการทำงานตามที่ได้รับมอบหมายจากผู้ว่าจ้าง

(2) การใช้ (Use)

วัตถุประสงค์ในการประมวลผลข้อมูลเพื่อประเมินความเสี่ยงก่อนรับงานสอบบัญชี

(3) การเปิดเผย (Disclosure)

กิจกรรมนี้ไม่มีการเปิดเผยไปยังบุคคลภายนอก เว้นแต่มีการตรวจสอบจากหน่วยงานที่เกี่ยวข้อง เช่น ที่ปรึกษาหรือผู้เชี่ยวชาญภายนอก เป็นต้น การเปิดเผยข้อมูลส่วนบุคคลที่ได้มาในกระบวนการนี้ จะต้องพิจารณาเปิดเผยภายใต้วัตถุประสงค์ และฐานกฎหมายที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล

(4) การเก็บรักษา (Storage/ Retention)

สำนักงานสอบบัญชี ควรพิจารณาบริหารจัดการ ดังนี้

- การจัดเก็บกรณีเป็นเอกสาร สำนักงานสอบบัญชีควรกำหนดผู้รับผิดชอบในการควบคุมดูแล รวมทั้งกำหนดนโยบายในการเข้าถึงข้อมูลที่จัดเก็บ และมีมาตรการจัดเก็บในตู้เอกสารที่ปิดล็อกได้

- การจัดเก็บกรณีเป็นไฟล์อิเล็กทรอนิกส์ ควรกำหนดผู้รับผิดชอบและกำหนดสิทธิการเข้าถึงของข้อมูล และทำการใส่รหัสเข้าไฟล์ เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ชอบด้วยกฎหมาย
- ในกรณีที่ได้รับข้อมูลส่วนบุคคลผ่านช่องทางไลน์ส่วนบุคคล (Line Chat) ควรพิจารณาลบข้อความเมื่อนำข้อมูลมาใช้แล้ว เพื่อป้องกันการรั่วไหลของข้อมูล
- มีการกำหนดระยะเวลาการจัดเก็บ โดยพิจารณาตามกฎหมาย ความจำเป็นในการจัดเก็บเพื่อบรรลุวัตถุประสงค์ในกิจกรรมนี้ เช่น การเก็บระยะเวลา 10 ปี ตามอายุความ กรณีเกิดข้อพิพาทขึ้นเก็บตลอดระยะเวลาตามที่กำหนดไว้ตามสัญญาเป็นต้น

(5) การทำลาย (Disposal)

กรณีไม่ผ่านประเมินความเสี่ยง ข้อมูลหมดความจำเป็นควรจะทำลายทิ้ง เว้นแต่ มีข้อกำหนดตามกฎหมายอื่น

กรณีผ่านการประเมินความเสี่ยง พิจารณาเก็บตามสัญญา เมื่อพ้นระยะเวลาในการเก็บรักษา หรือหมดความจำเป็นในการประมวลผล หรือเจ้าของข้อมูลใช้สิทธิในการขอให้ลบ สำนักงานมีหน้าที่ต้องดำเนินการทำลายข้อมูลส่วนบุคคลเหล่านั้น โดยวิธีการตามนโยบายของสำนักงานสอบบัญชีนั้น ๆ เช่น การย่อยเอกสาร การลบไฟล์ข้อมูลจากอีเมล คอมพิวเตอร์ หรือลบไฟล์ที่บักทึกบนระบบคลาวด์ (Cloud)

2. การรับงาน และการปฏิบัติงานสอบบัญชี

เมื่อตกลงรับทำงานสอบบัญชีกับลูกค้า (ผู้ว่าจ้าง) สำนักงานสอบบัญชี จะมีการจัดทำสัญญากับลูกค้า (Engagement) การติดต่อผู้สอบบัญชีรายเดิม (กรณีที่ลูกค้าเปลี่ยนผู้สอบบัญชี) และการวางแผนและออกแบบเพื่อทดสอบระบบการควบคุมภายในรวมถึงการวางแผนการตรวจสอบงบการเงินผู้สอบบัญชี จะมีการบันทึกข้อมูลในกระดาษทำการ และอาจมีการขอตัวอย่างเอกสารที่สุ่มตรวจและเก็บเอกสารไว้เป็นหลักฐาน

สิ่งที่เจ้าของสำนักงานสอบบัญชีควรระวังหรือพิจารณา ได้แก่

. **(1) การเก็บรวบรวมข้อมูล (Collection)**

กิจกรรมนี้มีการเก็บรวบรวม ประเภทของข้อมูลส่วนบุคคลและเอกสารที่เกี่ยวข้อง เช่น

- สำเนาบัตรประชาชนกรรมการ หุ้นส่วน ผู้มีอำนาจลงนามของบริษัท
- ชื่อ เบอร์ติดต่อ อีเมล ผู้ประสานงานของสำนักงานสอบบัญชี และผู้สอบบัญชีรายเดิม
- ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน เลขที่ผู้สอบบัญชีรับอนุญาตของบริษัท

- ชื่อ เบอร์ติดต่อ อีเมล ผู้ประสานงานของลูกค้า (ผู้ว่าจ้าง)
- ชื่อ เบอร์ติดต่อ อีเมล ผู้ประสานงานสำนักงานบัญชีของลูกค้า (ผู้ว่าจ้าง)
- ข้อมูลส่วนบุคคลอื่นที่เกี่ยวข้องกับงานสอบบัญชีตามมาตรฐานการสอบบัญชีทั้งภายในและภายนอก เช่น ลูกค้า คู่ค้า พนักงานของผู้ว่าจ้าง เป็นต้น

ข้อมูลส่วนบุคคลที่สำนักงานสอบบัญชีได้รับ เก็บรวบรวม และเปิดเผยข้อมูลเป็นการใช้ฐานสัญญาในการทำงานตามที่ได้รับมอบหมายจากผู้ว่าจ้าง

จากเอกสารข้างต้นจะมีข้อมูลส่วนบุคคลที่อ่อนไหว เช่น สำเนาบัตรประชาชน ประวัติสุขภาพ ประวัติอาชญากรรมของพนักงานผู้ว่าจ้างที่ได้รับเป็นเอกสารสำหรับประกอบการสอบบัญชี ซึ่งสำนักงานสอบบัญชีควรให้ลูกค้า (ผู้ว่าจ้าง) ดำเนินการปิดข้อมูลอ่อนไหว เช่น ศาสนา กรุ๊ปเลือด แต่ถ้าไม่ได้ดำเนินการมา สำนักงานสอบบัญชีอาจมีนโยบายในการปิดทับข้อมูลดังกล่าวเพื่อลดภาระในการจัดให้มีมาตรการเก็บรักษาข้อมูลส่วนบุคคลประเภทอ่อนไหว ซึ่งไม่ได้นำไปประมวลผลแต่อย่างใด

(2) การใช้ (Use)

วัตถุประสงค์ในการประมวลผลข้อมูลเพื่อปฏิบัติงานสอบบัญชี

(3) การเปิดเผย (Disclosure)

กิจกรรมนี้ไม่มีการเปิดเผยไปบุคคลภายนอก เว้นแต่มีกำหนดไว้ในกฎหมายอื่นๆ หรือหน่วยงานที่เกี่ยวข้อง การเปิดเผยข้อมูลส่วนบุคคลที่ได้มาในกระบวนการนี้ จะต้องพิจารณาเปิดเผยภายใต้วัตถุประสงค์ และฐานกฎหมายที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล

(4) การเก็บรักษา (Storage/ Retention)

สำนักงานสอบบัญชีควรดำเนินการดังนี้

- การจัดเก็บกรณีเป็นเอกสาร ทางสำนักงานสอบบัญชีควรกำหนดผู้รับผิดชอบในการควบคุมดูแล รวมทั้งกำหนดนโยบายในการเข้าถึงข้อมูลที่จัดเก็บ และมีมาตรการจัดเก็บในตู้เอกสารที่ปิดล็อกได้
- การจัดเก็บกรณีเป็นไฟล์อิเล็กทรอนิกส์ ควรกำหนดผู้รับผิดชอบและกำหนดสิทธิการเข้าถึงของข้อมูล และทำการใส่รหัสเข้าไฟล์ เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ชอบด้วยกฎหมาย
- ในกรณีที่ได้รับข้อมูลส่วนบุคคลผ่านช่องทางการสื่อสารส่วนบุคคล เช่น ไลน์ส่วนบุคคล (Line Chat) เมสเซนเจอร์ (Messenger) วอทแอพ (Whatsapp) เป็นต้น ควรพิจารณาลบข้อความเมื่อนำข้อมูลมาใช้แล้ว เพื่อป้องกันการรั่วไหลของข้อมูล

- ระยะเวลาการจัดเก็บ สำนักงานสอบบัญชีอาจเก็บตลอดระยะเวลาของสัญญาที่ให้บริการแก่บริษัทผู้ว่าจ้างได้ หรือพิจารณาเก็บตามระยะเวลาที่กฎหมายอนุญาตไว้ หรือตามความจำเป็นในการจัดเก็บเพื่อบรรลุวัตถุประสงค์ในกิจกรรมนี้ คือการเก็บข้อมูลเพื่อประโยชน์การสอบบัญชี ซึ่งเก็บตามกฎหมายที่เกี่ยวข้อง เช่น เก็บไม่น้อยกว่า 5 ปี ตามมาตรฐานการสอบบัญชีนับจากวันที่ในรายงานผู้สอบบัญชี เป็นต้น

(5) การทำลาย (Disposal)

เมื่อพ้นระยะเวลาในการเก็บรักษา หรือหมดความจำเป็นในการประมวลผล หรือเจ้าของข้อมูลใช้สิทธิในการขอให้ลบ สำนักงานมีหน้าที่ต้องดำเนินการทำลายข้อมูลส่วนบุคคลเหล่านั้น โดยวิธีการตามนโยบายของสำนักงานสอบบัญชีนั้น ๆ เช่น การย่อยเอกสาร การลบไฟล์ข้อมูลจากอีเมล คอมพิวเตอร์ หรือลบไฟล์ที่บักทึกบนระบบคลาวด์ (Cloud)

3. การจ้างบุคคลภายนอกเพื่อการปฏิบัติงานสอบบัญชี

ในการรับทำงานสอบบัญชีกับลูกค้า (ผู้ว่าจ้าง) ในบางธุรกิจที่เป็นงานเฉพาะและต้องอาศัยผู้เชี่ยวชาญที่รู้และเข้าใจในกระบวนการทำงานของธุรกิจ เช่น การจ้างผู้เชี่ยวชาญเฉพาะด้าน หรือผู้ช่วยผู้สอบบัญชีจากภายนอกเพื่อเป็นส่วนหนึ่งของงานสอบบัญชี

สิ่งที่เจ้าของสำนักงานสอบบัญชีควรระวังหรือพิจารณา ได้แก่

(1) การเก็บรวบรวมข้อมูล (Collection)

กิจกรรมนี้มีการเก็บรวบรวม ประเภทของข้อมูลส่วนบุคคลและเอกสารที่เกี่ยวข้อง เช่น

- สำเนาบัตรประชาชนของผู้เชี่ยวชาญ/ผู้ช่วยผู้สอบบัญชีที่ว่าจ้าง
- ชื่อ-นามสกุล เลขประจำตัวผู้เสียภาษี ของผู้เชี่ยวชาญ/ผู้ช่วยผู้สอบบัญชีที่ว่าจ้าง
- เลขที่บัญชีธนาคาร (ในกรณีการโอนค่าจ้างผ่านบัญชีธนาคาร)
- ประวัติการศึกษา ประวัติการทำงานของผู้เชี่ยวชาญที่ว่าจ้าง
- ชื่อ เบอร์ติดต่อ อีเมล ผู้เชี่ยวชาญ หรือผู้ช่วยผู้สอบบัญชีที่ว่าจ้าง
- ใบอนุญาตประกอบวิชาชีพเฉพาะทางของบุคคลภายนอกที่สำนักงานว่าจ้าง

ข้อมูลส่วนบุคคลที่สำนักงานสอบบัญชีได้เก็บรวบรวมจากผู้เชี่ยวชาญ/ผู้ช่วยผู้สอบบัญชีที่ว่าจ้าง เป็นการดำเนินการเพื่อปฏิบัติตามสัญญาว่าจ้าง จึงสามารถใช้ฐานการปฏิบัติตามสัญญาได้

ในกรณีที่มีข้อมูลส่วนบุคคลที่อ่อนไหว ควรมีการดำเนินการ ดังนี้ เอกสารสำเนาบัตรประชาชนของผู้เชี่ยวชาญ /ผู้ช่วยผู้สอบบัญชีที่ว่าจ้าง ปิดข้อมูล ศาสนาและกรุ๊ปเลือดมาให้ แต่ถ้าไม่ได้ดำเนินการมา สำนักสอบบัญชีควรต้องดำเนินการ

(2) การใช้ (Use)

วัตถุประสงค์ในการประมวลผลข้อมูลเพื่อการจ้างบุคคลภายนอกที่เกี่ยวข้องเพื่อการปฏิบัติงานสอบบัญชี

(3) การเปิดเผย (Disclosure)

การเปิดเผยข้อมูลส่วนบุคคลที่ได้มาในกระบวนการนี้ จะต้องพิจารณาเปิดเผยภายใต้วัตถุประสงค์ และฐานกฎหมายที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล การเปิดเผยในกิจกรรมนี้ส่วนใหญ่จะมีการเปิดเผยแก่บุคคลหรือหน่วยงานที่มีอำนาจตามที่กฎหมายกำหนด เช่น กรมสรรพากร กรณีของการนำส่งภาษีหัก ณ ที่จ่าย และหน่วยงานที่เกี่ยวข้อง เป็นต้น

(4) การเก็บรักษา (Storage/ Retention)

สำนักงานสอบบัญชีควรดำเนินการดังนี้

- การจัดเก็บกรณีเป็นเอกสาร สำนักงานสอบบัญชีควรกำหนดผู้รับผิดชอบในการควบคุมดูแล รวมทั้งกำหนดนโยบายในการเข้าถึงข้อมูลที่จัดเก็บ และมีมาตรการจัดเก็บในตู้เอกสารที่ปิดล็อกได้
- การจัดเก็บกรณีเป็นไฟล์อิเล็กทรอนิกส์ ควรกำหนดผู้รับผิดชอบและกำหนดสิทธิการเข้าถึงของข้อมูล และทำการใส่รหัสเข้าไฟล์ เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ชอบด้วยกฎหมาย
- ระยะเวลาการจัดเก็บ สำนักงานสอบบัญชีอาจเก็บตลอดระยะเวลาของสัญญาว่าจ้าง หรือพิจารณาเก็บตามระยะเวลาที่กฎหมายอนุญาตไว้ หรือตามความจำเป็นในการจัดเก็บเพื่อบรรลุวัตถุประสงค์ในกิจกรรมนี้ เช่น เก็บไม่น้อยกว่า 5 ปี ตามมาตรฐานการสอบบัญชี หรือเก็บระยะเวลา 10 ปี ตามอายุความของกฎหมายแพ่ง กรณีเกิดข้อพิพาทขึ้น เป็นต้น

(5) การทำลาย (Disposal)

เมื่อพ้นระยะเวลาในการเก็บรักษา หรือหมดความจำเป็นในการประมวลผล หรือเจ้าของข้อมูลใช้สิทธิในการขอให้ลบ สำนักงานมีหน้าที่ต้องดำเนินการทำลายข้อมูลส่วนบุคคลเหล่านั้น โดยวิธีการตามนโยบายของสำนักงานสอบบัญชีนั้น ๆ เช่น การย่อยเอกสาร การลบไฟล์ข้อมูลจากอีเมล คอมพิวเตอร์ หรือลบไฟล์ที่บักทึกบนระบบคลาวด์ (Cloud)

บทที่ 3 แนวทางด้านกระบวนการรองรับการใช้สิทธิ และการบริหารจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

3.1 แนวทางการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้เพื่อเป็นการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยประกอบด้วย 9 สิทธิ ได้แก่

สิทธิ	รายละเอียด
1. สิทธิในการถอนความยินยอม (Right to Withdraw Consent) ตาม มาตรา 19 วรรค 5	เจ้าของข้อมูลส่วนบุคคลต้องสามารถถอนความยินยอมด้วยวิธีที่ง่ายและสามารถถอนความยินยอมได้ตลอดเวลา สำนักงานต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอม โดยการถอนความยินยอมต้องไม่ส่งผลกระทบกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมในช่วงเวลาก่อนจะใช้สิทธิในการถอนความยินยอม และหากการเก็บรวบรวมข้อมูลส่วนบุคคลอยู่ในฐานอื่นๆ เจ้าของข้อมูลส่วนบุคคลจะไม่สามารถใช้สิทธิถอนความยินยอมได้ ประกอบด้วย ฐานสัญญา และฐานปฏิบัติตามกฎหมาย
2. สิทธิในการได้รับแจ้ง (Right to Be Informed) ตามมาตรา 23	ในการเก็บรวบรวมข้อมูลส่วนบุคคล สำนักงานต้องแจ้งรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล โดยรายละเอียดที่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล ประกอบด้วย วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล การแจ้งให้ทราบในกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล ประเภทหรือหน่วยงานที่เปิดเผยข้อมูลส่วนบุคคล และข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
3. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) ตามมาตรา 30	เจ้าของข้อมูลส่วนบุคคลสามารถขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนเองหรือขอให้มีการเปิดเผยที่มาของข้อมูลส่วนบุคคล โดยข้อมูลที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ออกเป็น 3 ส่วน ได้แก่ 1. ข้อมูลยืนยันว่าผู้ควบคุมข้อมูลส่วนบุคคลมีการประมวลผล

สิทธิ	รายละเอียด
	2. ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลนำมาใช้ในการประมวลผล 3. ข้อมูลอื่น อาทิ รายละเอียดการประมวลผล ที่มาของข้อมูลส่วนบุคคล สำนักงานต้องปฏิบัติตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยการจัดส่งข้อมูลตามคำขอใช้สิทธิผ่านช่องทางเดียวกับการยื่นคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น เจ้าของข้อมูลส่วนบุคคลยื่นคำขอผ่านทางรูปแบบอิเล็กทรอนิกส์ สำนักงานควรจัดส่งข้อมูลตามคำขอใช้สิทธิในรูปแบบอิเล็กทรอนิกส์
4. สิทธิในการโอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability) ตามมาตรา 31	เจ้าของข้อมูลส่วนบุคคลสามารถขอรับข้อมูลส่วนบุคคลของตนเองจากบริษัท โดยบริษัทต้องทำให้ข้อมูลอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานได้โดยทั่วไปด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานโดยอัตโนมัติ และเจ้าของข้อมูลมีสิทธิขอให้บริษัทโอนย้ายข้อมูลส่วนบุคคลของตนเองไปให้กับผู้ควบคุมข้อมูลอื่นซึ่งสามารถทำโดยวิธีการอัตโนมัติ
5. สิทธิในการคัดค้านประมวลผลข้อมูลส่วนบุคคล (Right to Object)ตามมาตรา 32	เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เกี่ยวข้องกับตนเอง สามารถแบ่งออกเป็น 3 กรณีดังต่อไปนี้ 1. กรณีมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยได้รับการยกเว้นไม่ต้องขอความยินยอม ยกเว้นสำนักงานสามารถแสดงให้เห็นว่าเป็นการปฏิบัติตามกฎหมาย 2. กรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์การตลาดแบบตรง (Direct Marketing) 3. กรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ยกเว้นเป็นการดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
6. สิทธิในการลบข้อมูลส่วนบุคคล (Right to Erasure) ตามมาตรา 33	เจ้าของข้อมูลส่วนบุคคลสามารถขอให้บริษัทดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม (Anonymization) โดยการทำให้ข้อมูลส่วนบุคคลนั้น ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้
7. สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล (Right to	เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล แบ่งออกเป็น 4 กรณีดังต่อไปนี้

สิทธิ	รายละเอียด
Restrict Processing) ตามมาตรา 34	1. กรณีผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบข้อมูลเพื่อแก้ไขให้ถูกต้อง 2. กรณีผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการลบหรือทำลายข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลขอให้มีการระงับการใช้ข้อมูล 3. กรณีข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ในการเก็บ 4. กรณีเจ้าของข้อมูลส่วนบุคคลอยู่ในกระบวนการที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการขอใช้สิทธิคัดค้านการใช้ข้อมูลส่วนบุคคล
8. สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to Rectification) ตามมาตรา 36	เจ้าของข้อมูลส่วนบุคคลสามารถขอให้บริษัทแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และตามมาตรา 36 หากบริษัทไม่สามารถดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล จะต้องมีการบันทึกเหตุในการปฏิเสธลงในการบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) (ศึกษาเอกสารตัวอย่างเพิ่มเติมได้ที่ บทที่ 5 ข้อ 5.1)
9. สิทธิในการร้องเรียน (Right to Lodge a Complaint) ตาม มาตรา 73	เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ซึ่งแต่งตั้งโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

สำนักงานมีหน้าที่ต้องกำหนดแนวปฏิบัติให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้ ในกรณีที่สำนักงานสอบบัญชี มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในกิจกรรมที่มีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล มีหน้าที่ต้องสร้างแนวปฏิบัติการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรการการใช้สิทธิของข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ สำนักงานสอบบัญชี ประกอบด้วย 2 ประเภท ได้แก่

1. เจ้าของข้อมูลส่วนบุคคลภายในองค์กร เช่น พนักงานหรือบุคลากร ผู้บริหารหรือกรรมการและผู้ถือหุ้นของบริษัท เป็นต้น

2. เจ้าของข้อมูลส่วนบุคคลภายนอกองค์กร เช่น ลูกค้า คู่ค้า คู่สัญญา ที่ปรึกษา ผู้รับจ้างช่วง บุคคลที่มีความเกี่ยวข้องกับการดำเนินงาน เป็นต้น

ขั้นตอนสำหรับการการปฏิบัติหน้าที่ของสำนักงานสอบบัญชี เมื่อเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิ

(1) การเตรียมแบบฟอร์มและช่องทางรับรองใช้สิทธิ

ในการยื่นคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลสำนักงานสอบบัญชี อาจจัดให้มีได้หลายรูปแบบ เช่น ทางอิเล็กทรอนิกส์ (อีเมลหรือเว็บไซต์) ทางวาจา (โทรศัพท์ หรือ ต่อหน้าบุคคล) ลายลักษณ์อักษร โดยสำนักงานสอบบัญชี ควรมีการจัดทำแบบฟอร์มคำขอ เพื่อทราบรายละเอียดตัวบุคคลที่ยื่นคำขอ และข้อมูลที่จำเป็นต่อการติดต่อกลับ การกำหนดแบบฟอร์มคำขอควรหลีกเลี่ยงไม่ให้เกิดการขอข้อมูลส่วนบุคคลที่บริษัทได้จัดเก็บไปแล้ว โดยอาจเก็บเฉพาะชื่อนามสกุล และรหัสประจำตัวประชาชน ซึ่งเป็นข้อมูลที่เพียงพอต่อการนำไปค้นหาข้อมูลทั้งหมดในฐานข้อมูล กรณีผู้ใช้สิทธิไม่ใช่เจ้าของข้อมูลส่วนบุคคล บริษัทต้องแบ่งพื้นที่ให้กรอกข้อมูลของผู้ทรงสิทธิ กับผู้ยื่นคำขอแยกออกจากกัน

บริษัทต้องดำเนินการจัดเตรียมแบบคำขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำขอใช้สิทธิได้ผ่านช่องทางต่างๆ ดังตัวอย่างต่อไปนี้

ช่องทางยื่นคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล	ช่องทางการใช้สิทธิ	ฝ่ายที่รับผิดชอบ
1. บุคคลภายในสำนักงาน เช่น • พนักงานหรือบุคลากรภายในสำนักงาน • ผู้บริหารหรือกรรมการบริษัท • ผู้ถือหุ้นของบริษัท	ช่องทางที่ฝ่ายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จัดเตรียมไว้ หรือช่องทางที่สำนักงานกำหนด	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสารตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่ตั้งขึ้นเพื่อดำเนินการ
2. บุคคลภายนอกสำนักงาน เช่น • ลูกค้า • คู่ค้า คู่สัญญา • บุคคลที่มีความเกี่ยวข้องกับการดำเนินงาน	1. Application 2. Website 3. ติดต่อกับสำนักงานโดยตรง (Walk in) 4. โทรศัพท์	อาจแต่งตั้งผู้รับผิดชอบด้านข้อมูลส่วนบุคคล เพื่อตรวจสอบเอกสารตรวจสอบการยืนยันตัวตน จากนั้นจึงส่งเรื่องต่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ที่ตั้งขึ้นเพื่อดำเนินการ

ในการยื่นคำขอสำนักงานสอบบัญชี ควรจัดสรรช่องทางตามประเภทของเจ้าของข้อมูลส่วนบุคคลข้างต้น สำนักงานควรมีการแจ้งช่องทางการใช้สิทธิเพื่อให้เจ้าของข้อมูลทราบ โดยต้องแจ้งในประกาศความเป็นส่วนตัว (Privacy notice) ตามกลุ่มของเจ้าของข้อมูล และจะต้องมีการจัดเตรียมความพร้อม เกี่ยวกับกระบวนการดำเนินการขอใช้สิทธิ

(2) ตรวจสอบตัวตนของผู้ยื่นคำขอ

สำนักงานสอบบัญชีต้องตรวจสอบตัวตนของผู้ยื่นคำขอ โดยในกรณีที่เป็นเจ้าของข้อมูลยื่นคำขอด้วยตนเอง ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุตัวตนว่าเป็นเจ้าของข้อมูลจริง

ในกรณีที่ผู้ยื่นคำขอเป็นบุคคลอื่น ต้องพิจารณาต่อไปว่าบุคคลดังกล่าวเป็นบุคคลที่มีอำนาจทำแทนเจ้าของข้อมูลส่วนบุคคลหรือไม่ โดยอาจพิจารณาจากเอกสารหนังสือมอบอำนาจ (กรณีมอบอำนาจ) ที่ได้มีการแนบตอนยื่นเอกสารขอใช้สิทธิ

เมื่อสำนักงานสอบบัญชี ได้ดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว สำนักงานควรพิจารณา เก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับการพิจารณายืนยันตัวตน เช่น วัน เวลา รูปแบบคำขอ ผลสำเร็จในการตรวจสอบตัวตน เพื่อเป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบตัวตนของสำนักงานหากเกิดกรณีมีการฟ้องร้องคดีในอนาคต

สำนักงานสอบบัญชี ควรหลีกเลี่ยงวิธีการยืนยันตัวตนด้วยการขอให้เจ้าของข้อมูลส่วนบุคคลยื่นสำเนาบัตรประจำตัวประชาชนประกอบกับคำขอ เพราะสำเนาบัตรประจำตัวประชาชนได้รวบรวมข้อมูลส่วนบุคคลไว้หลายประการ รวมถึงข้อมูลศาสนาซึ่งเป็นข้อมูลอ่อนไหว ในกรณีสำนักงานจำเป็นต้องใช้สำเนาบัตรประชาชนเพื่อยืนยันตัวตน สำนักงานควรจัดเตรียมมาตรการที่จำเป็นในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล และอาจทำลายเอกสารหลังจากที่เจ้าหน้าที่ได้ดำเนินการยืนยันตัวตน รวมถึงอาจมีการปิดทับข้อมูลศาสนา ซึ่งเป็นข้อมูลอ่อนไหวในสำเนาบัตรประชาชนหรือเอกสารอื่นที่ใช้ในการยืนยันตัวตน เพื่อไม่เป็นการเพิ่มภาระให้กับสำนักงาน

(3) พิจารณาความถูกต้องของคำขอ

เมื่อผู้รับผิดชอบด้านข้อมูลส่วนบุคคล ได้รับคำขอแล้วและยืนยันตัวตนแล้วว่าเจ้าของข้อมูลส่วนบุคคลเป็นผู้ยื่นคำขอจริง สำนักงานต้องนำคำขอมาพิจารณาต่อไปว่า คำขอใช้สิทธินั้นสำนักงานมีเหตุปฏิเสธสิทธิได้หรือไม่ โดยสำนักงานสามารถปฏิเสธได้หากเข้าข้อใดข้อหนึ่งใน 3 กรณี ดังต่อไปนี้

1) กรณีที่ข้อมูลในคำขอไม่เป็นตามเงื่อนไขที่กำหนดในการใช้สิทธิ เช่น ยื่นเอกสารไม่ครบตามที่กำหนด การเขียนรายละเอียดในแบบคำขอผิด เป็นต้น

2) กรณีที่มีข้อยกเว้นการใช้สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น สิทธิการเข้าถึง (Right of access) มาตรา 30 ได้กำหนดเหตุแห่งการปฏิเสธไว้ในกรณีที่เป็นการปฏิเสธตามคำสั่งศาลหรือตามกฎหมาย และ การเข้าถึงหรือขอรับสำเนานั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิเสรีภาพของบุคคล

3) กรณีข้อยกเว้นตามกฎหมายเฉพาะ โดยกฎหมายเฉพาะได้มีการบัญญัติห้ามแจ้งให้เจ้าของข้อมูลส่วนบุคคลไม่ให้สามารถใช้สิทธิได้ เช่น กรณีพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ 2542 มาตรา 21/1 ได้บัญญัติว่า

“ห้ามมิให้ผู้มีหน้าที่รายงานตามมาตรา 13 และมาตรา 16 หรือบุคคลใดเปิดเผยข้อมูลหรือกระทำด้วยประการใด ๆ อันอาจทำให้ลูกค้าหรือบุคคลภายนอกทราบเกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า การรายงานธุรกรรมหรือการส่งข้อมูลอื่นใดไปยังสำนักงาน เว้นแต่เป็นการปฏิบัติตามกฎหมายหรือตามคำสั่งศาลหรือเป็นการเปิดเผยข้อมูลระหว่างสำนักงานใหญ่กับสาขาของผู้มีหน้าที่รายงานตามมาตรา 13 และมาตรา 16 ที่ตั้งอยู่ในหรือต่างประเทศเพื่อดำเนินการอันเกี่ยวเนื่องกับการปฏิบัติตามพระราชบัญญัตินี้”

รายงานที่สำนักงานได้รับตามหมวดนี้ถือเป็นความลับในราชการเกี่ยวกับการดำเนินการตามพระราชบัญญัตินี้และให้เลขาธิการสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เป็นผู้รับผิดชอบในการจัดเก็บรักษาและใช้ประโยชน์จากข้อมูลดังกล่าวเฉพาะเพื่อการปฏิบัติการตามพระราชบัญญัติ

(4) แจ้งผลการพิจารณาดำเนินการตามสิทธิที่ร้องขอ

สำนักงานสอบบัญชีต้องแจ้งให้ผู้ยื่นคำขอทราบ ไม่ว่าจะพิจารณาว่าจะดำเนินการหรือไม่ดำเนินการ กรณีที่สำนักงานสอบบัญชี พิจารณาว่าจะดำเนินการตามคำขอ ควรกำหนดระยะเวลาให้ชัดเจนให้เจ้าของข้อมูลส่วนบุคคลทราบว่าจะดำเนินการให้แล้วเสร็จภายในวันใด โดยเกณฑ์ดังกล่าวเป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด และในกรณีที่มีความจำเป็นต้องขยายระยะเวลาจากกรอบเวลาเดิมนับแต่วันที่มีการยื่นคำขอ ทั้งนี้ตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

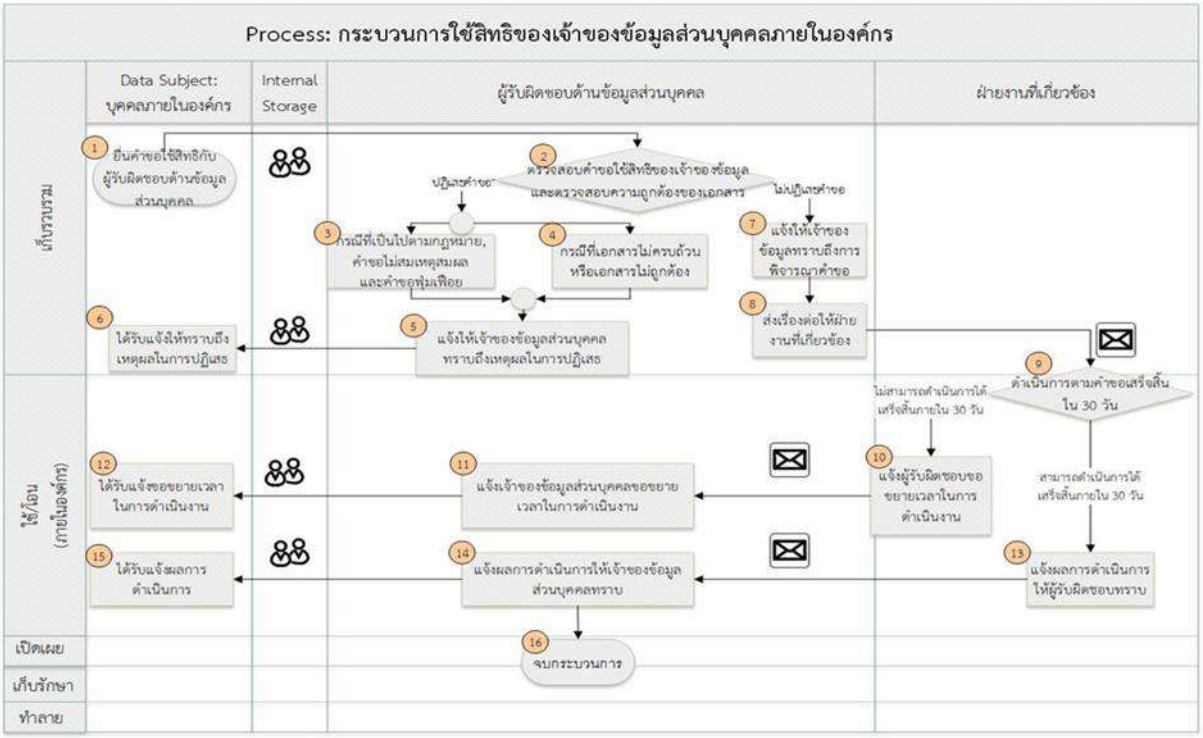
ในส่วนของค่าใช้จ่ายในการดำเนินการกฎหมายไทยยังไม่มีการกำหนดระยะเวลาที่ชัดเจน ทั้งนี้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

กรณีที่สำนักงานสอบบัญชี พิจารณาว่าจะไม่ดำเนินการตามคำขอจะต้องระบุข้อเท็จจริงกับเหตุผลที่ทำให้ปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลให้ชัดเจน

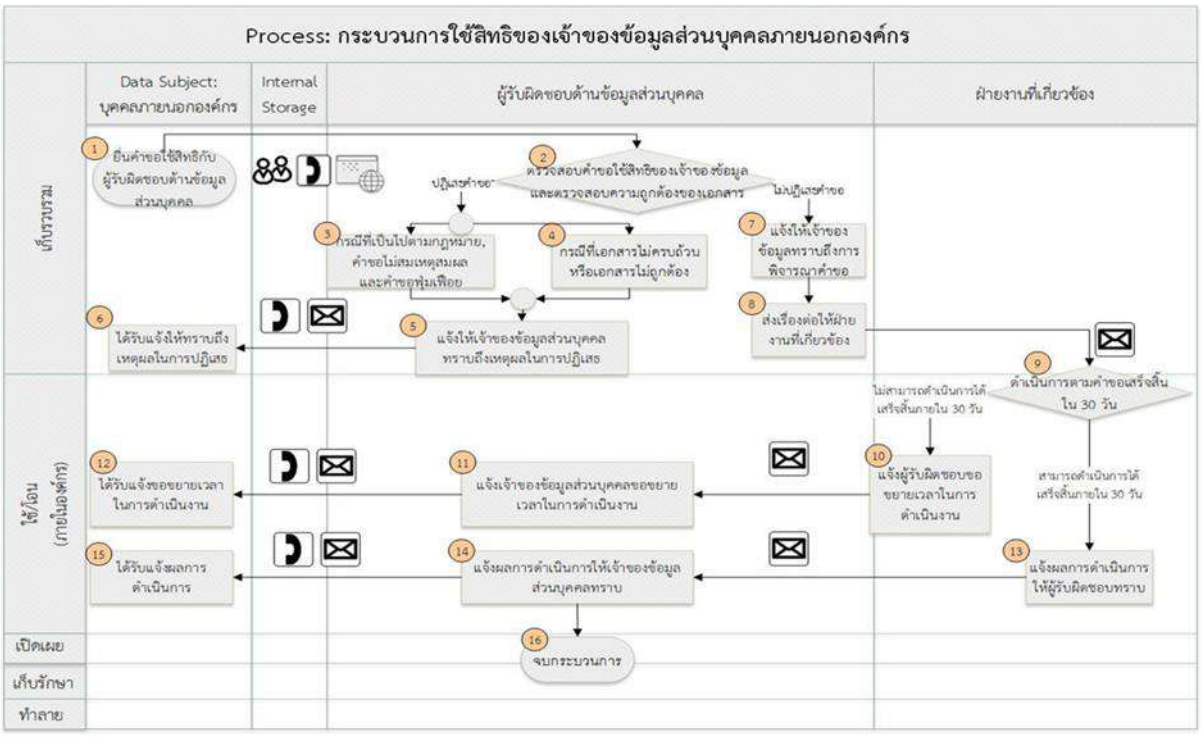
(5) รวบรวมข้อมูลที่ได้รับการร้องเรียนให้ชี้แจงและดำเนินการตามสิทธิที่ร้องขอ

เมื่อพิจารณาแล้วสำนักงานสอบบัญชีเห็นว่าต้องดำเนินการตามคำขอ ฝ่ายที่รับผิดชอบเกี่ยวกับการดำเนินการใช้สิทธิต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อแจ้งและดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล เมื่อได้ดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเรียบร้อย ควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบผ่านช่องทางติดต่อที่เจ้าของข้อมูลส่วนบุคคลยื่นขอใช้สิทธิ เช่น ทาง SMS หรือ E-Mail เป็นต้น รายละเอียดในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ประกอบด้วย รายละเอียดการติดต่อของเจ้าหน้าที่ดูแลข้อมูลส่วนบุคคล ผลการดำเนินงานตามคำขอของเจ้าของข้อมูลส่วนบุคคล เหตุผลการปฏิเสธการดำเนินการตามคำขอ และช่องทางการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงช่องทางการติดต่อให้บุคคลภายนอกสำนักงานทราบ นอกจากนั้นสำนักงานต้องบันทึกรายละเอียดในการดำเนินการต่างๆ ในแบบบันทึกรายการเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล ทั้งการดำเนินการตามคำขอใช้สิทธิเรียบร้อยแล้วหรือการปฏิเสธคำขอตามหลักเกณฑ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้โดยสามารถบันทึกเป็นหนังสือหรือผ่านช่องทางอิเล็กทรอนิกส์ดังตัวอย่างแบบบันทึกรายการเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง แผนผังกระบวนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายในองค์กร



ตัวอย่าง แผนผังกระบวนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายนอกองค์กร



ตัวอย่าง แบบบันทึกรายการเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

รายละเอียดการยื่นและรับคำขอใช้สิทธิ					รายการคำขอ	รายละเอียดการพิจารณา	วันที่	เวลา	ผู้พิจารณา	บทกฎหมายที่เกี่ยวข้อง	ผลการพิจารณา	เหตุผลในการปฏิเสธ
ลำดับ	วันที่	เวลา	ผู้ยื่นคำขอ	ผู้รับคำขอ								

3.2 แนวทางการแจ้งเหตุข้อมูลรั่วไหล (Data Breach Management)

สำนักงานสอบบัญชี มีกิจกรรมที่มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีหน้าที่ในการจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม และควรกำหนดมาตรการแจ้งเหตุข้อมูลรั่วไหล ตามมาตรา 37(4) เพื่อเตรียมความพร้อมและเตรียมตัวรับมือกับการรั่วไหลของข้อมูลส่วนบุคคล เช่น ข้อมูลถูกลักลอบคัดลอกออกไปภายนอกโดยอดีตพนักงาน และเอกสารในรูปแบบกระดาษที่มีรายการข้อมูลส่วนบุคคลถูกโจรกรรม เป็นต้น ควรมีการดำเนินการเพื่อเตรียมรับมือกับภัยคุกคามหรือเกิดการละเมิดข้อมูลส่วนบุคคลที่จะเกิดขึ้น ได้แก่

1. จัดเตรียมขั้นตอนและวิธีการในการแจ้งเหตุข้อมูลรั่วไหล
2. สื่อสารให้บุคลากรภายในองค์กรเข้าใจ
3. จัดเตรียมแบบตัวอย่างการแจ้งเหตุข้อมูลรั่วไหล
4. ซักซ้อมวิธีการตามแผนที่กำหนด เพื่อเตรียมความพร้อมและให้บุคลากรในองค์กรสามารถรับมือกับเหตุการณ์ที่เกิดขึ้นได้

สำนักงานสอบบัญชี ควรมีแนวทางหรือกระบวนการในการจัดการเมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคล เนื่องจากหากไม่มีการแจ้งเมื่อเกิดการละเมิดข้อมูลส่วนบุคคลอย่างเหมาะสมและภายในระยะเวลาที่กฎหมายกำหนด อาจได้รับผลกระทบทางกฎหมาย และยังส่งผลกระทบไปยังเจ้าของข้อมูลส่วนบุคคล ที่อาจสูญเสียความเป็นส่วนตัว ถูกจำกัดสิทธิเสรีภาพ ถูกเลือกปฏิบัติ ถูกฉ้อโกง ถูกโจรกรรมข้อมูลระบุตัวตน สูญเสียทรัพย์สิน หรือเสียชีวิต เป็นต้น

ในการดำเนินการแจ้งเหตุข้อมูลรั่วไหล ดำเนินการดังต่อไปนี้

1) ทำความเข้าใจว่าอะไรคือเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

เหตุละเมิดข้อมูลส่วนบุคคลเป็นการกระทำ หรือเหตุการณ์ด้านความปลอดภัยที่ส่งผลต่อการรักษาความลับ ความสมบูรณ์ หรือความพร้อมใช้ของข้อมูลส่วนบุคคล ยกตัวอย่าง เช่น การสูญเสียการควบคุมข้อมูลส่วนบุคคล การถูกจำกัดสิทธิและเสรีภาพ การถูกเข้าถึงข้อมูลโดยมิชอบโดยบุคคลอื่นที่ไม่มีอำนาจ การส่งข้อมูลส่วนบุคคลไปยังผู้รับที่ไม่ถูกต้อง การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเสียเปรียบทางเศรษฐกิจหรือสังคม เป็นต้น นอกจากนี้ยังมีกรณีที่เกี่ยวกับอุปกรณ์หรือการละเมิดข้อมูลทางกายภาพ เช่น อุปกรณ์คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลถูกขโมยหรือสูญหาย เป็นต้น

สิ่งสำคัญที่ต้องคำนึงถึงคือ เหตุละเมิดมีแนวโน้มว่าจะเกิดความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหรือไม่

ในบางกรณีการละเมิดข้อมูลไม่ได้หมายความเฉพาะที่มีผลกระทบต่อระบบความปลอดภัย หรือการสูญเสีย การควบคุมข้อมูล การถูกจำกัดสิทธิในการเข้าถึงข้อมูลเท่านั้น อาจหมายความรวมถึงกรณีที่เกิดกับบุคคลโดยได้รับผลกระทบเป็นสภาพจิตใจ อารมณ์ เป็นต้น ซึ่งผู้ประเมินความเสี่ยงจะต้องพิจารณาจากปัจจัยที่อาจจะเกี่ยวข้องทั้งหมด และเป็นการพิจารณารายกรณีไป

2) เมื่อเกิดเหตุข้อมูลรั่วไหล บุคคลที่เกี่ยวข้องคือใครบ้าง : ผู้มีหน้าที่แจ้งและผู้มีหน้าที่รับแจ้ง

(1) ผู้มีหน้าที่แจ้ง : ผู้ควบคุมข้อมูลส่วนบุคคล

สำนักงานสอบบัญชี มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามมาตรา 37(4) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคลมีหน้าที่ประเมินความเสี่ยงว่าข้อมูลส่วนบุคคลที่รั่วไหลดังกล่าวส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือไม่อย่างไร เพื่อพิจารณาการแจ้งเหตุข้อมูลส่วนบุคคลรั่วไหลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล ต่อไป

(2) ผู้มีหน้าที่แจ้ง : ผู้ประมวลผลข้อมูลส่วนบุคคล

สำนักงานสอบบัญชี มีบทบาทเป็นผู้ประมวลผลข้อมูลส่วนบุคคลเอง ตามมาตรา 40(2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุข้อมูลรั่วไหลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบในกรณีที่เกิดภัยคุกคามหรือเกิดการละเมิดข้อมูลส่วนบุคคล แต่ไม่ได้มีหน้าที่แจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการแจ้งและประสานการละเมิดข้อมูลส่วนบุคคล

(3) ผู้มีหน้าที่รับแจ้ง : สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เป็นหน่วยงานกำกับดูแลที่ทำหน้าที่ในการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

3) ประเมินความเสี่ยงเหตุการณ์รั่วไหลข้อมูล

เมื่อเกิดเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคล สำนักงานสอบบัญชีควรประเมินระดับความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล สำหรับพิจารณาเพื่อแจ้งต่อหน่วยงานที่กำกับดูแลตามกฎหมาย ซึ่งคือ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล

การประเมินระดับความเสี่ยง ประกอบด้วยปัจจัยที่ต้องนำมาพิจารณาเพื่อเป็นส่วนหนึ่งของการประเมินความเสี่ยง ดังต่อไปนี้

(1) ข้อมูลส่วนตัวถูกเข้ารหัสหรือไม่

(2) ถ้ามีการเข้ารหัส เป็นการเข้ารหัสที่ยากใช่หรือไม่

(3) ข้อมูลแฝงอยู่ในขอบเขตใด เช่น สามารถระบุตัวบุคคลได้จากข้อมูล

(4) ชื่อ ที่อยู่ รายละเอียดลักษณะทางกายภาพ

(5) ปริมาณข้อมูลที่เกี่ยวข้อง

(6) จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ

(7) ลักษณะของการละเมิด เช่น การโจรกรรม การสร้างความเสียหายโดยไม่ตั้งใจ

(8) ปัจจัยอื่นๆ ที่เกี่ยวข้อง

การให้เหตุผลและการหาข้อสรุปวิธีการประเมินความเสี่ยง ควรได้รับการบันทึกไว้อย่างครบถ้วนและลงนามเห็นชอบโดยผู้บริหารระดับสูง โดยผลลัพธ์ของการประเมินความเสี่ยงควรมีข้อสรุปอย่างใดอย่างหนึ่ง ดังต่อไปนี้

1. การละเมิดข้อมูลส่วนบุคคลไม่จำเป็นต้องดำเนินการใดๆ

2. การละเมิดข้อมูลส่วนบุคคลจำเป็นต้องมีการแจ้งเตือนต่อหน่วยงานที่กำกับดูแล ได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3. การละเมิดข้อมูลส่วนบุคคลจำเป็นต้องมีการแจ้งเตือนต่อหน่วยงานที่กำกับดูแล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) และเจ้าของข้อมูลส่วนบุคคล

โดยสิ่งที่สำนักงานสอบบัญชี ควรดำเนินการ ดังนี้

1. กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรม แบบฟอร์มในการแจ้ง ดังตัวอย่างแบบฟอร์มหนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและกระบวนการการดำเนินการแจ้งเหตุละเมิดให้แก่ตัวแทนของสำนักงานให้ชัดเจน เช่นการส่งอีเมล และแจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

2. กำหนดวิธีการปฏิบัติให้ตัวแทนสำนักงานต้องดำเนินการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

3. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเข้าของข้อมูลส่วนบุคคล

ดังนั้นสำนักงานสอบบัญชี สามารถดำเนินการแจ้งเหตุข้อมูลรั่วไหล โดยพิจารณาจากการประเมินความเสี่ยงเพื่อดำเนินการแจ้งต่อหน่วยงานกำกับดูแลตามกฎหมาย

4) เกณฑ์การพิจารณาเพื่อจะแจ้งต่อหน่วยงานที่กำกับดูแล และ เจ้าของข้อมูล

(1) กรณีต้องแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อมีการประเมินระดับความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเรียบร้อยแล้ว และพบว่าต้องมีการตัดสินใจที่จะแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 37(4) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่มีเหตุผลที่ถูกต้องตามกฎหมายที่ทำให้ไม่สามารถแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลได้ในระยะเวลาที่กำหนด

การแจ้งเหตุการณ์รั่วไหลของข้อมูลควรมีรายละเอียดการแจ้งมีดังต่อไปนี้

1. คำอธิบายลักษณะของการรั่วไหลของข้อมูล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง
2. ประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคล
3. วิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4. คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว
5. คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น
6. รายละเอียดอื่น ๆ เพิ่มเติมตามความเหมาะสม

ดังนั้น สำนักงานสอบบัญชีที่มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคล ควรมีการประเมินระดับความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และหากพบว่าการรั่วไหลมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล สำนักงานสอบบัญชี ต้องแจ้งเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

(2) กรณีต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคล

สำนักงานสอบบัญชีที่มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่มีการประเมินความเสี่ยงการรั่วไหลของข้อมูลส่วนบุคคล และพบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและ

เสรีภาพของเจ้าของข้อมูลส่วนบุคคล จะต้องมีการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ

การพิจารณาเพื่อแจ้งต่อเจ้าของข้อมูลส่วนบุคคล ตามมาตรา 37(4) กำหนดไว้ว่า

ผู้ควบคุมข้อมูลส่วนบุคคลควรแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา เมื่อการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล การประเมินความเสี่ยงที่ได้ดำเนินการก่อนขั้นตอนการพิจารณาเพื่อแจ้งเจ้าของข้อมูลส่วนบุคคลจะต้องมีการพิจารณาความเสี่ยงต่อสิทธิและเสรีภาพของข้อมูลที่ได้รับผลกระทบ หากพบว่าข้อมูลที่ถูกละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลควรมีการดำเนินการแจ้งไปยังเจ้าของข้อมูลส่วนบุคคล

ดังนั้น สำนักงานสอบบัญชี มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องการดำเนินการพิจารณาความเสี่ยงต่อสิทธิและเสรีภาพของข้อมูลที่ได้รับผลกระทบ

หากพบว่าข้อมูลที่ถูกละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลควรมีการดำเนินการแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลด้วยวิธีดำเนินการตามความเหมาะสม

วิธีแจ้งเตือนเจ้าของข้อมูลส่วนบุคคล

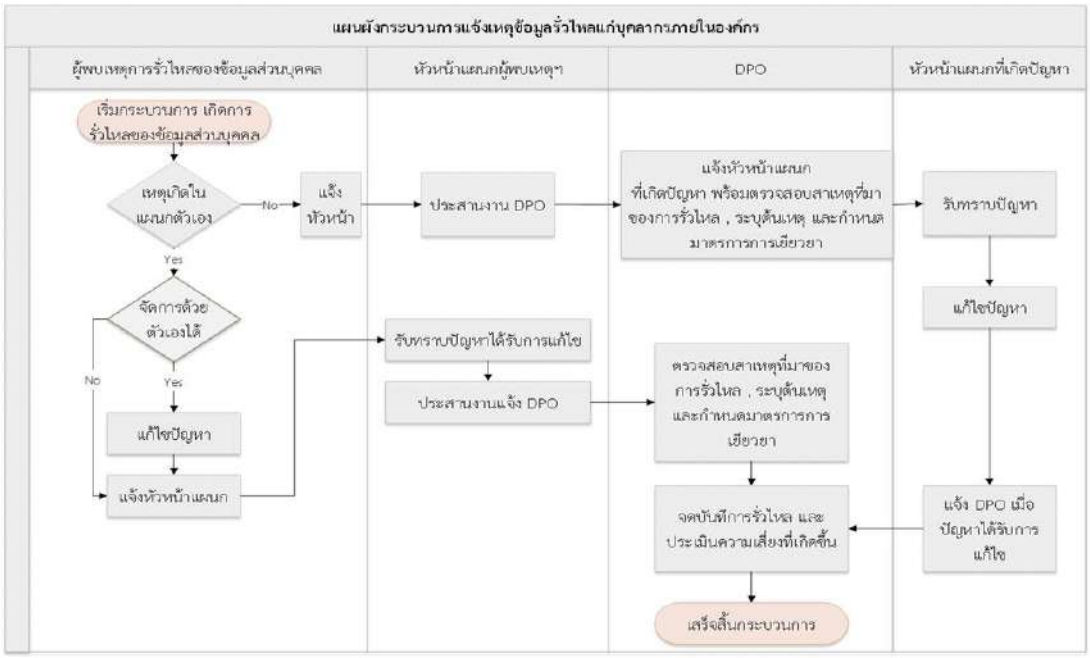
ตามมาตรา 37 (4) เมื่อมีการตัดสินใจแล้วว่าการมีการละเมิดข้อมูลจะแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลโดยไม่ล่าช้า โดยอธิบายลักษณะของการละเมิดข้อมูลส่วนบุคคลพร้อมกับแนวทางการเยียวยาอย่างชัดเจนและต้องครอบคลุมถึงรายละเอียด ดังต่อไปนี้

1. คำอธิบายลักษณะของการรั่วไหลของข้อมูล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง
2. ประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคล
3. วิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4. คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว
5. คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น
6. คำอธิบายของมาตรการที่ใช้หรือเสนอเพื่อดำเนินการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลรวมถึงมาตรการบรรเทาผลกระทบที่อาจเกิดขึ้นตามความเหมาะสม
7. รายละเอียดอื่น ๆ เพิ่มเติมตามความเหมาะสม

นอกเหนือจากที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนด ผู้ควบคุมข้อมูลส่วนบุคคลอาจมีการให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการกระทำต่างๆ เพื่อช่วยให้สามารถลดความเสี่ยงที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล

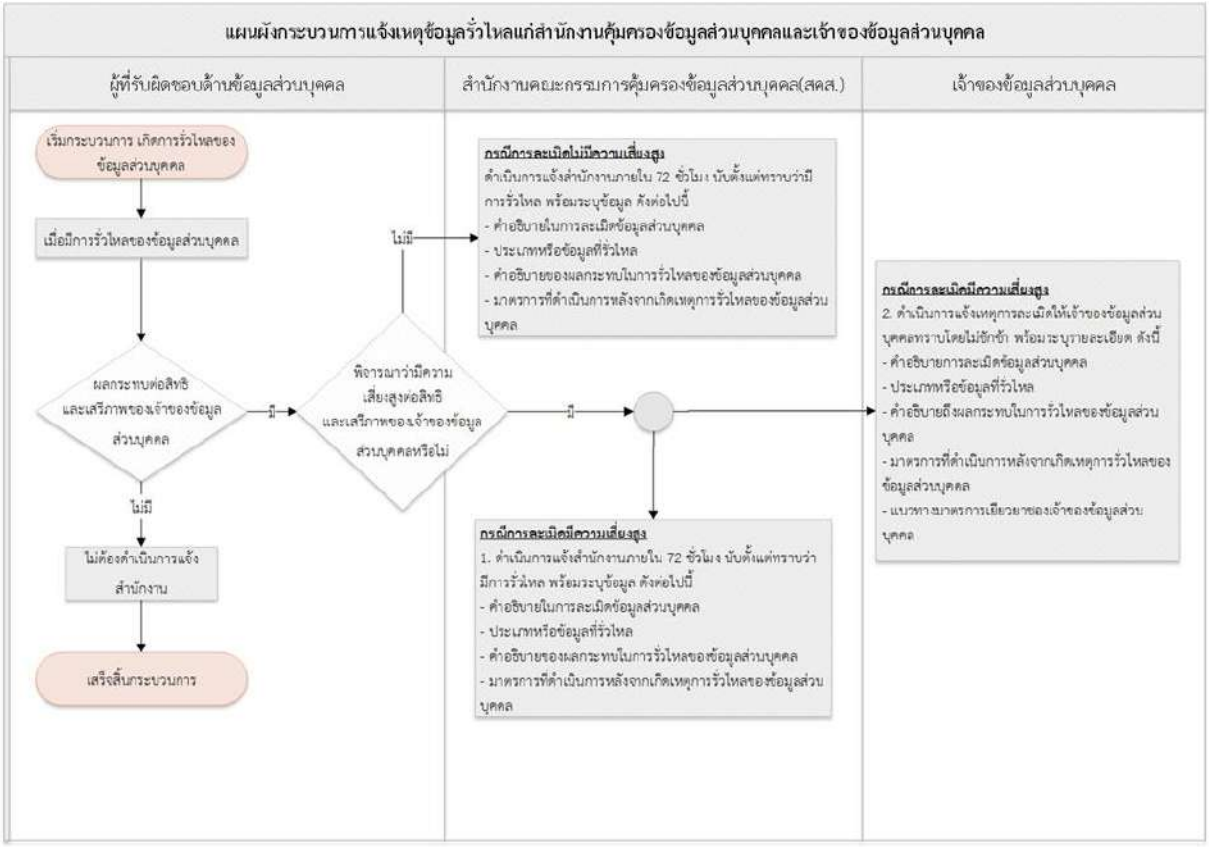
การแจ้งเตือนไปยังเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบนั้นไม่ได้ถูกกำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังนั้น ในกรณีที่พิจารณาว่าการละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีนี้อาจใช้รูปแบบการสื่อสารสาธารณะ หรืออาจเปลี่ยนแปลงตามข้อเสนอแนะของหน่วยงานที่กำกับดูแลและข้อมูลเพิ่มเติมอย่างต่อเนื่อง และหากพิจารณาว่าการละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล อาจใช้รูปแบบการสื่อสารที่มีความเฉพาะเจาะจงและมีความรวดเร็วในการสื่อสาร เช่น โทรศัพท์ เป็นต้น

ตัวอย่าง แผนผังกระบวนการแจ้งเหตุข้อมูลรั่วไหลแก่บุคคลภายในองค์กร



ตัวอย่าง

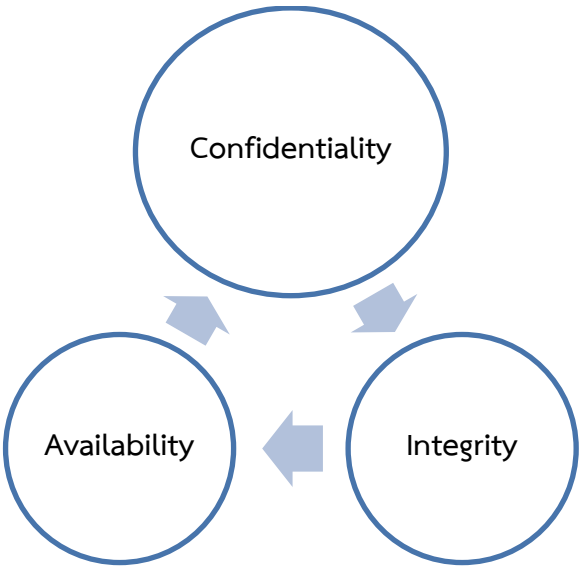
แผนผังกระบวนการแจ้งเหตุข้อมูลรั่วไหลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล



บทที่ 4 แนวทางด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เป็นมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลควรกำหนดและมีการดำเนินการอย่างเหมาะสม เพื่อสร้างแนวทางป้องกันการประมวลผลข้อมูลส่วนบุคคลจากบุคคลที่ไม่ได้รับอนุญาต ตามมาตรา 37 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดไว้ว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ และต้องมีการทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

โดยการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Personal Data Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต



มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ อย่างน้อยต้องมีการดำเนินการดังต่อไปนี้

1. มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

2. มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

3. มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

4. มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

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) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

6. มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่าง

เหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

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

(2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (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) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(3) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(4) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

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

และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

แนวทางเบื้องต้นในการรักษาความมั่นคงปลอดภัยของข้อมูลในสำนักงาน

การดำเนินการในการประกอบธุรกิจ ไม่ว่าจะเป็นธุรกิจสำนักงานสอบบัญชีในปัจจุบัน ต่างมีการนำเทคโนโลยีเข้ามาปรับใช้ในการทำงาน เพื่ออำนวยความสะดวกให้การดำเนินการเป็นไปอย่างรวดเร็ว ประหยัดเวลาและเปิดโอกาสในการสร้างงานสร้างรายได้มากยิ่งขึ้น ทั้งนี้ การนำเทคโนโลยีเข้ามาปรับใช้ก็เป็นดาบสองคม ที่มีทั้งข้อดีในเรื่องการอำนวยความสะดวกในการทำงาน และก็นำมาซึ่งความเสี่ยงในการคุ้มครองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลมากยิ่งขึ้น แต่อย่างไรก็ตามหากสำนักงานเข้าใจวิธีการใช้เทคโนโลยีอย่างมีความปลอดภัยมากขึ้น ความเสี่ยงในการเกิดเหตุรั่วไหลของข้อมูลย่อมลดน้อยลง โดยในแนวปฏิบัติฉบับนี้ จะเสนอแนวทางเบื้องต้นในการรักษาความมั่นคงปลอดภัยของข้อมูลในสำนักงาน ดังนี้

1) การใช้งานคอมพิวเตอร์ส่วนบุคคล

การใช้งานเครื่องคอมพิวเตอร์ควรมีการกำหนดรหัสผ่าน (Password) ก่อนการเข้าสู่การใช้งานคอมพิวเตอร์ เพื่อความปลอดภัยของข้อมูลและป้องกันคนอื่นเข้าสู่เครื่องคอมพิวเตอร์ของเราอย่างง่ายดาย

ขั้นตอนการกำหนดรหัสผ่าน (Password)

1. รหัสที่ใช้ควรมีการกำหนดอย่างน้อย 8 ตัวอักษร ประกอบด้วยอักษรเล็ก อักษรใหญ่ ตัวเลขและอักขระพิเศษปนอยู่ด้วย
2. รหัสควรเปลี่ยนทุก 3 เดือน
3. รหัสควรเก็บไว้เป็นความลับไม่บอกใครและไม่ควรแปะไว้ที่หน้าจอคอมพิวเตอร์

การจัดเก็บไฟล์ข้อมูล

การจัดเก็บไฟล์ข้อมูลต่างๆ ถือเป็นส่วนที่สำคัญมาก เพราะเป็นการเข้าถึงข้อมูลโดยตรง ดังนั้นจึงควรระวังการเข้าถึงข้อมูลในไฟล์เป็นอย่างมาก วิธีการป้องกันการเข้าถึงข้อมูลได้แก่ การล็อกโฟลเดอร์ การเข้ารหัสไฟล์ จัดเก็บข้อมูลบนคลาวด์ เป็นต้น

(1) การจัดเก็บข้อมูลบนคอมพิวเตอร์

ทำการติดตั้งโปรแกรมที่ใช้ในการล็อกโฟล์เดอร์ หรือ ไฟล์ข้อมูล บนเครื่องคอมพิวเตอร์ จากนั้นทำการกำหนดพาสเวิร์ดตามขั้นตอนการกำหนดพาสเวิร์ด

(2) การจัดเก็บข้อมูลบนคลาวด์

เป็นการจัดเก็บข้อมูลบนไดรฟ์ที่ผู้ให้บริการคลาวด์ มีให้ใช้งานทั้งแบบฟรี และแบบเสียค่าใช้จ่าย การเก็บข้อมูลบนคลาวด์ ช่วยในการป้องกันการเข้าถึงข้อมูลได้ในระดับหนึ่งอย่างง่าย ที่สามารถเริ่มต้นทำได้ โดยไม่เสียค่าใช้จ่ายเพิ่มเติม เช่น Google Microsoft เป็นต้น ทั้งนี้ ในการจัดเก็บข้อมูลบนคลาวด์ มีขั้นตอนเบื้องต้น

1. เข้าสู่ระบบผู้ให้บริการคลาวด์ หลังจากเข้าสู่ระบบแล้ว จะมีการสอบถามให้บันทึกรหัสผ่าน (Password) ไหม ระมัดระวังการตั้งค่ากำหนดจำรหัสผ่าน (Password)

2. สร้างโฟลเดอร์แยกเป็นหมวดหมู่ เพื่อทำการจัดเก็บข้อมูลเป็นสัดส่วน

3. ทำการอัปโหลดไฟล์ขึ้นระบบคลาวด์

4. ออกจากระบบคลาวด์ อย่าล็อกอินทิ้งไว้ เพื่อป้องกันบุคคลอื่นสามารถเข้าเครื่องคอมพิวเตอร์ได้ จะไม่สามารถเข้าถึงระบบคลาวด์ได้ทันที

(3) การจัดเก็บข้อมูลบนแหล่งเก็บข้อมูลเคลื่อนที่

การจัดเก็บข้อมูลบนแหล่งเก็บข้อมูลเคลื่อนที่ คือการจัดเก็บข้อมูลลงอุปกรณ์ต่าง ๆ ที่สามารถพกพาไปที่อื่นได้ นอกเหนือจากเครื่องคอมพิวเตอร์ เช่น ทรัมไดรฟ์ ฮาร์ดดิสก์พกพา หรือ สมาร์ทโฟน เป็นต้น

ขั้นตอนการจัดเก็บข้อมูลบนแหล่งเก็บข้อมูลเคลื่อนที่

1. กรณีจัดเก็บข้อมูลบนฮาร์ดดิสก์หรือทรัมไดรฟ์พกพา ให้ติดตั้งโปรแกรมรหัสผ่าน (Password) เพื่อป้องกันการเข้าถึงอุปกรณ์ได้โดยตรงทันทีที่เสียบต่อเข้าตรงกับคอมพิวเตอร์ ซึ่งโปรแกรมเหล่านี้ ปัจจุบันมีแถมมากับอุปกรณ์ฮาร์ดดิสก์และทรัมไดรฟ์ จึงสามารถติดตั้งและกำหนดรหัสผ่าน (Password) ในการเข้าถึงไดรฟ์ได้เลยทันที โดยหลักการกำหนดรหัสผ่าน (Password) ให้ดูจากขั้นตอนการกำหนดรหัสผ่าน (Password) ข้างต้น

2. กรณีจัดเก็บข้อมูลลงบนอุปกรณ์มือถือ ให้จัดเก็บข้อมูลลงใน โฟลเดอร์ที่ปลอดภัย (Secure Folder) ซึ่งปัจจุบันมีการให้บริการนี้บนมือถืออยู่แล้ว และกำหนดพาสเวิร์ดในการเข้าถึงอุปกรณ์มือถือ เพื่อป้องกันการเข้าถึงอุปกรณ์มือถือได้อย่างง่าย และควรกำหนดตัวเลขในการเข้าถึงอุปกรณ์มือถือเป็นตัวเลขจำนวน 6 หลัก หรือจากลายนิ้วมือ

การลบทำลายไฟล์ข้อมูล

การลบไฟล์ข้อมูลหรือทำลายไฟล์ข้อมูลกรณีที่ไม่ได้ใช้งานแล้ว แต่ในไฟล์ดังกล่าวปรากฏข้อมูลส่วนบุคคลอยู่ จึงมีความจำเป็นที่จะต้องลบข้อมูลทิ้งอย่างถาวร เพื่อไม่ให้หลงเหลือไว้ถังขยะ (Recycle Bin) เป็นการป้องกันการกู้ข้อมูลที่พ้นระยะเวลาการเก็บหรือหมดความจำเป็นกลับมาใช้ได้อีกต่อไป

ขั้นตอนการลบข้อมูลทิ้งอย่างถาวร

1. เลือกไฟล์ที่ต้องการลบ จากนั้นกด Shift+Delete จะปรากฏกล่องข้อความสอบถามต้องการลบข้อมูลอย่างถาวรใช่หรือไม่ ให้เลือกว่าใช่ จากนั้นไฟล์ข้อมูลจะถูกลบอย่างถาวร ไม่ถูกเก็บไว้ในถังขยะ

2. กรณีที่คลิกขวาที่ไฟล์แล้วเลือก Delete หรือ กดปุ่ม Delete บนแป้นพิมพ์ ให้ไปที่ถังขยะแล้วเลือกไฟล์ที่ต้องการลบข้อมูลทิ้ง และกดลบอีกครั้งหนึ่ง เพื่อป้องกันบุคคลอื่นเข้าไปกู้ไฟล์ขึ้นมาแล้วนำมาใช้งานหรือเปิดอ่านได้อีกครั้งหนึ่ง

2) การใช้งานคอมพิวเตอร์ในระบบเน็ตเวิร์ค (Network)

การใช้งานในระบบเครือข่ายเน็ตเวิร์ค เป็นการใช้งานคอมพิวเตอร์แบบแชร์ทรัพยากรการใช้งาน การใช้งานแบบนี้มีความเสี่ยงเป็นอย่างมากในการที่ใครก็ตามที่อยู่ในระบบเครือข่ายสามารถเข้าถึงข้อมูลได้ทันที หากไม่ได้กำหนดสิทธิการเข้าถึงไว้อย่างชัดเจน

(1) กำหนดให้มีการเข้าสู่ระบบด้วยระบบโดเมนเนม

การเข้าสู่ระบบเครือข่ายด้วยระบบโดเมนเนมนั้น เป็นรูปแบบการเข้าสู่ระบบเครือข่ายแบบการยืนยันตัวตนเข้าสู่ระบบการใช้งานและตรวจสอบว่ามีสิทธิ์การเข้าใช้งานในทรัพยากรไหนได้บ้าง อีกทั้งยังช่วยป้องกันบุคคลภายนอกหรืออุปกรณ์การเข้าถึงเครือข่ายเข้ามาภายในระบบโดยไม่ได้รับอนุญาตอีกด้วย

(2) กำหนดโฟลเดอร์การเข้าถึงการใช้งานตามหน่วยงานหรือแผนก

หลังจากที่เข้าสู่ระบบด้วยระบบโดเมนเนม ระบบจะทราบว่าใครคือผู้เข้ามาในระบบเครือข่าย ทำงานแผนกไหน เกี่ยวข้องและจำเป็นต้องเข้าถึงข้อมูลส่วนไหนบ้าง ให้แอดมินผู้ดูแลระบบเครือข่าย กำหนดและจำกัดสิทธิในการเข้าถึงข้อมูลไฟล์ต่าง ๆ ออกเป็นโฟลเดอร์ เพื่อการบริหารจัดการการเข้าถึงข้อมูลที่ง่าย และไม่ยุ่งยาก

(3) กำหนดสิทธิ์ของผู้เข้าใช้งานในการกระทำกับข้อมูลไฟล์ในโฟลเดอร์

ผู้ที่เข้ามาในระบบเครือข่ายอาจมีได้หลายแผนกและหลายส่วนงาน แต่ไม่ใช่ทุกคนที่สามารถทำการคัดลอกข้อมูล แก้ไข หรือ ลบไฟล์ได้ ให้แอดมินผู้ดูแลระบบ กำหนด

สิทธิ์ในการใช้ไฟล์ข้อมูลในโฟลเดอร์นั้นๆ เพื่อเป็นการป้องกันการนำข้อมูลออกไปใช้แก้ไขข้อมูล ที่อาจส่งผลให้เกิดความผิดพลาดของข้อมูลได้ และทำการลบข้อมูลผู้ใช้งานออก เมื่อพ้นสภาพหรือไม่มีความจำเป็นต้องเข้าถึงข้อมูล ดังนั้นข้อมูลส่วนนี้ถือว่ามีความสำคัญและจำเป็นอย่างมากที่ต้องปรับปรุงให้ใหม่อยู่เสมอ

(4) จัดเก็บ Log การเข้าใช้งานของผู้ใช้งานบนเครือข่ายทั้งหมด

เป็นการจัดเก็บบันทึกข้อมูลผู้ใช้งานในระบบเครือข่ายว่ามีผู้ใช้งานคนไหน เข้ามาใช้งานเข้าถึงไฟล์ข้อมูลต่างๆ แก้ไข ลบข้อมูลไฟล์ต่างๆ ในระบบเครือข่ายทั้งหมดบ้าง เพื่อจะได้รับรู้ถึงการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูล และสามารถตรวจสอบได้เมื่อพบว่าไฟล์ข้อมูลนั้นมีปัญหา

(5) กำหนดการลบข้อมูลบนทรัพยากรส่วนกลางให้เป็นแบบถาวร

การลบข้อมูลบนทรัพยากรกลางก็เหมือนกับการลบข้อมูลบนคอมพิวเตอร์ส่วนบุคคล ซึ่งจะไม่ได้ทำการลบข้อมูลทิ้งไปเลยทีเดียว แต่จะมีการนำไปไว้ที่ถังขยะก่อน ดังนั้น ผู้ดูแลระบบควรกำหนดรูปแบบการลบข้อมูลบนทรัพยากรส่วนกลางให้เป็นแบบถาวร เพื่อจะได้ไม่สามารถทำการกู้ไฟล์ขึ้นมาได้อีก

บทที่ 5 แนวทางในการจัดทำเอกสารเพื่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้ถูกตราขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการในการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้กฎหมายดังกล่าวได้กำหนดบทบาทหน้าที่แก่บุคคลซึ่งมีส่วนเกี่ยวข้องในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือเรียกรวมกันว่า การประมวลผลข้อมูล เช่น ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น โดยบทบาทหน้าที่ตามที่กฎหมายกำหนดนำมาซึ่งการจัดทำเอกสารเพื่อบรรลุหน้าที่ในการปฏิบัติตามกฎหมายดังกล่าว โดยเฉพาะผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล จำเป็นที่จะต้องดำเนินการตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนด

ทั้งนี้ เอกสารที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล แล้วแต่กรณี จะต้องดำเนินการ อย่างน้อยควรประกอบไปด้วยเอกสารดังต่อไปนี้ ซึ่งในส่วนนี้ได้ยกตัวอย่างแนวทางในการจัดเอกสารดังกล่าวเพื่อให้องค์กรสามารถนำไปปรับ ประยุกต์ใช้กับบริบทขององค์กรตนเองต่อไป

- ☑ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities)
- ☑ ประกาศความเป็นส่วนตัว (Privacy Notice)
- ☑ หนังสือขอความยินยอม (Consent Form)
- ☑ แบบคำขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request)
- ☑ ข้อตกลงประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)
- ☑ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Notifications)

5.1 บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities)

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ให้ผู้ประกอบการซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล จะต้องจัดทำบันทึกรายการ และในกรณีที่ผู้ประกอบการมีบทบาทเป็นผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลด้วยเช่นกัน โดยในส่วนนี้จะอธิบายเกี่ยวกับการจัดทำบันทึกรายการทั้ง 2 แบบ ดังนี้

1) การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

กฎหมายกำหนดรายละเอียดของบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเอาไว้ ดังนี้

(1) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ชื่อ และรายละเอียดการติดต่อขององค์กร รวมถึง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ได้แก่ คำอธิบายเกี่ยวกับหมวดหมู่ของเจ้าของข้อมูลส่วนบุคคล (categories of individual) หรือหมวดหมู่ข้อมูลส่วนบุคคล (categories of personal data) ที่องค์กรทำการประมวลผล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม กล่าวคือ หากองค์กรใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 องค์กรต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39 ด้วย ซึ่งในทางปฏิบัติหมายความถึง

(1) ให้ระบุฐานทางกฎหมายในการประมวลผล และ

(2) ให้ระบุการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก

(7) การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามมาตรา 30 วรรคสาม (สิทธิในการเข้าถึง) มาตรา 31 วรรคสาม (สิทธิในการ

ขอให้โอนข้อมูล) มาตรา 32 วรรคสาม (สิทธิในการคัดค้านการประมวลผล) และมาตรา 36 วรรคหนึ่ง (สิทธิในการขอแก้ไขข้อมูลให้ถูกต้อง) ตามเงื่อนไขที่กฎหมายกำหนด

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

อย่างไรก็ตาม กฎหมายไม่ได้กำหนดรูปแบบตายตัวในการจัดทำบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคล เพียงแต่ต้องจัดทำเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ แต่จะต้องจัดทำในลักษณะที่สามารถแก้ไข ปรับปรุงได้ เช่น การใช้โปรแกรม Microsoft Excel หรือ Software อื่นๆ ที่รองรับการบันทึกรายการดังกล่าว เป็นต้น

<u>ตัวอย่าง</u> บันทึกรายการ (Record of Processing Activities: RoPA)

สำหรับผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 1 ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล	
ผู้ควบคุมข้อมูลส่วนบุคคล	
ชื่อองค์กร	*สำนักสอบบัญชี เอบีซี*
ที่อยู่	*เลขที่.... อาคาร..... แขวง..... เขต..... กรุงเทพมหานคร*
อีเมล	*info@ABCAudit.com*
เบอร์โทรศัพท์	*02-000 000*
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (ถ้ามี)	
ชื่อ-สกุล	*นายปกป้อง คุ้มครอง*
ที่อยู่	*เลขที่.... อาคาร..... แขวง..... เขต..... กรุงเทพมหานคร*
อีเมล	*DPO@ABCAudit.com*
เบอร์โทรศัพท์	*02-000 001*

ส่วนที่ 2 บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล									
กิจกรรม	วัตถุประสงค์ในการประมวลผลข้อมูล	ประเภทของเจ้าของข้อมูล	ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	ฐานกฎหมาย	การเปิดเผยข้อมูลแก่บุคคลภายนอก	ระยะเวลาการเก็บรักษาข้อมูล	รูปแบบการเก็บรักษาข้อมูล	ผู้มีสิทธิ์เข้าถึงข้อมูล	มาตรการรักษาความมั่นคงปลอดภัย
คำอธิบาย: ระบุชื่อกิจกรรมซึ่งเกิดขึ้นจากการประกอบธุรกิจ หรือการดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	คำอธิบาย: ระบุวัตถุประสงค์หลักในการประมวลผลข้อมูลส่วนบุคคลในแต่ละ โดยเป็นเหตุผลหลักที่ต้องเก็บรวบรวม ใช้ เปิดเผยข้อมูลในกิจกรรมนั้น	คำอธิบาย: ระบุประเภทบุคคลซึ่งเป็นเจ้าของข้อมูลที่ข้อมูลนั้นสามารถบ่งชี้ไปถึง	คำอธิบาย: ระบุประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมในกิจกรรมนั้น ๆ	คำอธิบาย: ระบุฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูล ตามมาตรา 24และ 26	คำอธิบาย: ระบุประเภทบุคคลภายนอกที่อาจเปิดเผยข้อมูลส่วนบุคคลนั้นไปในแต่ละกิจกรรม	คำอธิบาย: ระบุระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล ว่าจะเก็บไว้เป็นระยะเวลานานเพียงใด	คำอธิบาย: ระบุรูปแบบหรือระบบในการเก็บรักษาข้อมูล	คำอธิบาย: ระบุบุคคลผู้มีสิทธิหรือมีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้	คำอธิบาย: ระบุมาตรการรักษาความมั่นคงปลอดภัย ซึ่งใช้ในการดูแลข้อมูลส่วนบุคคลในกิจกรรมนั้นๆ
ตัวอย่าง *การสรรหาพนักงาน*	*เพื่อพิจารณาคัดเลือกบุคคลเข้าเป็นพนักงาน*	*ผู้สมัครงาน*	*1.ชื่อ-สกุล 2.ที่อยู่-เบอร์ติดต่อ 3.ประวัติการศึกษา 4.....*	*ฐานการปฏิบัติตามสัญญา*	*ไม่มี*	*1 ปี นับแต่วันที่ทราบผลการคัดเลือก*	*กระดาษ : เก็บไว้ในตู้ล็อกเอกสารในสำนักงาน ไฟล์: บันทึกบนคลาวด์*	*หัวหน้าสำนักงาน และบุคคลที่หัวหน้าสำนักงานมอบหมายเท่านั้น*	*1. เก็บในตู้ล้อก ที่หัวหน้าสำนักงานเป็นผู้รักษากุญแจ 2. เก็บไว้บนคลาวด์ ที่กำหนดสิทธิเฉพาะหัวหน้าสำนักงานเท่านั้น*

ส่วนที่ 3 บันทึกรายการการปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคล						
เลขที่คำขอ	วันที่รับคำขอ	ผู้ยื่นคำขอ	รายละเอียดคำขอ	เหตุแห่งการปฏิเสธสิทธิ	วันที่แจ้งปฏิเสธสิทธิ	หมายเหตุ
001	*01/06/2565*	*นายสอบ ซื่อตรง*	*ขอเข้าถึงเอกสารข้อมูลส่วนบุคคลของ นาย ข.*	*ไม่สามารถดำเนินการตามคำขอได้ เนื่องจากไม่ใช่เจ้าของข้อมูลส่วนบุคคล และไม่ได้รับมอบอำนาจจากเจ้าของข้อมูลให้เข้าถึงข้อมูลได้*	*02/06/2565*	*-*

2) การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีผู้ประมวลผลข้อมูลส่วนบุคคล กฎหมายกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องควบคุมและป้องกันไม่ให้ผู้ประมวลผลข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ และให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

รายละเอียดของบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคลถูกกำหนดไว้ในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3 ดังนี้

(1) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลและตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(2) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูล ส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(3) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมถึงสถานที่ติดต่อและวิธีการติดต่อในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(4) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับ มอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(5) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(6) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 40 วรรคหนึ่ง (2)

การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสามารถช่วยสร้างความชัดเจนเกี่ยวกับขอบเขตของหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลและลดความเสี่ยงในการทำกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกเหนือขอบเขตที่ตกลงไว้กับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่ภาระในการปฏิบัติตามกฎหมายที่สูงมากขึ้น

ในส่วนของรูปแบบการบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคลนั้น กฎหมายไม่ได้มีรูปแบบตายตัว เพียงแต่ต้องจัดทำเป็นลายลักษณ์

อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ ทั้งนี้ รูปแบบการทำบันทึกดังกล่าวจะต้องแก้ไข เปลี่ยนแปลง และเข้าถึงได้ง่าย ดังนั้น การทำบันทึกในรูปแบบไฟล์อิเล็กทรอนิกส์ผ่านโปรแกรมพื้นฐาน เช่น MS Excel เป็นต้น

<u>ตัวอย่าง</u> บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

(Record of Processing Activities: RoPA) สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ส่วนที่ 1 ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล	
ผู้ประมวลผลข้อมูลส่วนบุคคล	
ชื่อ-สกุล/ชื่อองค์กร	*สำนักงานสอบบัญชี เอบีซี*
ที่อยู่	*เลขที่.... อาคาร..... แขวง..... เขต..... กรุงเทพมหานคร*
อีเมล	*info@ABCAudit.com*
เบอร์โทรศัพท์	*02-000 000*
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) **(ถ้ามี: กรณีผู้ประมวลผลข้อมูลแต่งตั้ง DPO)**	
ชื่อ-สกุล	*นายปกป้อง คุ้มครอง*
ที่อยู่	*เลขที่.... อาคาร..... แขวง..... เขต..... กรุงเทพมหานคร*
อีเมล	*DPO@ ABCAudit.com*
เบอร์โทรศัพท์	*02-000 001*

ส่วนที่ 2 บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล					
	ชื่อองค์กร	**ที่อยู่**		**อีเมล**	**เบอร์โทรศัพท์**
ผู้ควบคุมข้อมูลส่วนบุคคล	*บริษัท 123*	*เลขที่.... แขวง..... เขต..... กรุงเทพมหานคร*		*Info@123Corp.com*	*02-000-000*
กิจกรรม	วัตถุประสงค์ในการประมวลผลข้อมูล	ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	การเปิดเผยข้อมูลแก่บุคคลภายนอก	การเปิดเผยข้อมูลส่วนบุคคลไปต่างประเทศ	มาตรการรักษาความมั่นคงปลอดภัย
<u>คำอธิบาย:</u> ระบุชื่อกิจกรรม ซึ่งเกิดขึ้นจากการประกอบธุรกิจ หรือการดำเนินการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล	<u>คำอธิบาย:</u> ระบุวัตถุประสงค์หลักในการประมวลผลข้อมูลส่วนบุคคลในแต่ละ โดยเป็นเหตุผลหลักที่ต้องเก็บรวบรวม ใช้ เปิดเผยข้อมูลในกิจกรรมนั้น	<u>คำอธิบาย:</u> ระบุประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมในกิจกรรมนั้น ๆ	<u>คำอธิบาย:</u> ระบุประเภทบุคคลภายนอกที่อาจเปิดเผยข้อมูลส่วนบุคคลนั้นไปในแต่ละกิจกรรม	<u>คำอธิบาย</u> ระบุประเทศ และ/หรือ องค์กรที่ได้รับการเปิดเผยข้อมูลส่วนบุคคล	<u>คำอธิบาย:</u> ระบุมาตรการรักษาความมั่นคงปลอดภัย ซึ่งใช้ในการดูแลข้อมูลส่วนบุคคลในกิจกรรมนั้นๆ
<u>ตัวอย่าง</u> *งานจัดทำเงินเดือน (Payroll) พนักงานบริษัท 123*	*เพื่อจัดทำเงินเดือนพนักงานของบริษัทผู้ว่าจ้าง*	*1. ชื่อ-สกุล พนักงาน* *2. อัตราเงินเดือน* *3. เลขที่บัญชีธนาคาร* *4. .....*	*1. ธนาคาร* *2. สำนักงานประกันสังคม* *3. ผู้สอบบัญชี*	*ไม่มี*	*จัดเก็บข้อมูลพนักงานในรูปแบบไฟล์อิเล็กทรอนิกส์ โดยจัดเก็บไว้บนคลาวด์ ซึ่งกำหนดสิทธิเข้าถึง (access control) แก่ระดับหัวหน้าสำนักงาน และนักบัญชีผู้รับผิดชอบเท่านั้น*

5.2 ประกาศความเป็นส่วนตัว (Privacy Notice)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคล มีหน้าที่ในการแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล ตามมาตรา 23 ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล ยกเว้นในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดในการประมวลผลข้อมูลส่วนบุคคลนั้นอยู่แล้ว

การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 23 อย่างน้อยต้องประกอบไปด้วยรายละเอียด ดังต่อไปนี้

(1) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และฐานอำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคล

(2) การปฏิบัติตามกฎหมาย สัญญา หรือการแจ้งรายละเอียดประโยชน์โดยชอบด้วยกฎหมาย

(3) ประเภทของข้อมูลส่วนบุคคลและระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล

(4) ประเภทของผู้รับข้อมูล ในกรณีที่มีการส่งข้อมูลส่วนบุคคลให้กับบุคคลที่สาม

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

การแจ้งรายละเอียดของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลข้างต้นอาจอยู่ในรูปแบบใดก็ได้ กฎหมายไม่ได้กำหนดรูปแบบตายตัว อาจทำได้หลายวิธี ทั้งการทำเป็นหนังสือลายลักษณ์อักษร ทางวาจา หรือสื่ออิเล็กทรอนิกส์ เช่น ข้อความ SMS อีเมล เป็นต้น โดยอาจแจ้งข้อมูลเบื้องต้นแบบสั้นและจัดทำเป็นลิงก์หรือ QR Code เชื่อมโยงไปเว็บไซต์เพื่อแจ้งรายละเอียดที่ครบถ้วนตามที่กฎหมายกำหนดอีกชั้นหนึ่ง

ทั้งนี้ ประกาศความเป็นส่วนตัว สามารถพิจารณาจัดทำแยกเป็นฉบับเฉพาะสำหรับเจ้าของข้อมูลส่วนบุคคลแต่ละประเภทแยกออกจากกันได้ เช่น ประกาศความเป็นส่วนตัวสำหรับลูกค้า ประกาศส่วนตัวสำหรับพนักงาน เป็นต้น หรือจะจัดทำฉบับเดียวครอบคลุมเจ้าของข้อมูลส่วนบุคคลทุกประเภทก็สามารถกระทำได้ อย่างไรก็ตามการจัดทำประกาศความเป็นส่วนตัวสำหรับเจ้าของข้อมูลส่วนบุคคลแต่ละประเภทแยกออกจากกัน จะช่วยให้เจ้าของข้อมูลส่วนบุคคลประเภทนั้นๆ เข้าใจถึงรายละเอียดในการประมวลผลข้อมูลส่วนบุคคลของตนได้มากกว่า รวมทั้งลดความสับสน และหลีกเลี่ยงการแจ้งรายละเอียดวัตถุประสงค์ในการประมวลผลอื่นๆ ซึ่งไม่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลประเภทนั้น ๆ โดยต่อไปนี้จะยกตัวอย่างประกาศความเป็นส่วนตัว เพื่อนำไปปรับใช้เป็นประกาศความเป็นส่วนตัวสำหรับเจ้าของข้อมูลส่วนบุคคลแต่ละประเภทต่อไป

ตัวอย่าง

ประกาศความเป็นส่วนตัว (Privacy Notice)

บริษัท สอบบัญชี จำกัด (“บริษัท”) ตระหนักถึงความสำคัญและหน้าที่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยให้ความสำคัญในการเคารพสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และมุ่งมั่นเป็นอย่างยิ่งที่จะคุ้มครองข้อมูลส่วนบุคคลของท่านให้มีความปลอดภัย และเพื่อให้เกิดความมั่นใจว่าข้อมูลส่วนบุคคลของท่านจะได้รับความคุ้มครองตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้องกำหนด บริษัทจึงได้จัดทำประกาศความเป็นส่วนตัวฉบับนี้ขึ้น เพื่อแจ้งให้ทราบถึงรายละเอียดที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผย (รวมเรียกว่า **“การประมวลผล”**) รวมถึงสิทธิตามกฎหมายในฐานะเจ้าของข้อมูลส่วนบุคคล โดยมีรายละเอียดดังต่อไปนี้

ข้อ 1. ข้อมูลส่วนบุคคล หมายถึง

1.1 “ข้อมูลส่วนบุคคล” (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล ชื่อเล่น ที่อยู่ หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) เลขที่อยู่ไอพี (IP Address) คุกกี้ ไอดี (Cookie ID) เป็นต้น

1.2 “ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน” (Sensitive data) หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งบริษัทต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ โดยบริษัทจะเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อน ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากท่าน หรือในกรณีที่บริษัทมีความจำเป็นต้องดำเนินการตามที่กฎหมายอนุญาต

ข้อ 2. ข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม

บริษัท ได้จัดเก็บข้อมูลส่วนบุคคลของท่านเท่าที่จำเป็น ตามวัตถุประสงค์ในการใช้ข้อมูลที่บริษัทจะแจ้งให้ทราบในลำดับถัดไป ทั้งนี้ได้จำแนกประเภทของข้อมูลส่วนบุคคลที่บริษัทจัดเก็บไว้ ดังนี้

ประเภทของข้อมูล	<u>ตัวอย่าง</u>ข้อมูลที่บริษัทเก็บรวบรวม ใช้ และ/หรือ เปิดเผย
1) ข้อมูลส่วนตัว	(โปรดระบุ) เช่น ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน เลขที่หนังสือเดินทาง เลขประจำตัวผู้เสียภาษี เป็นต้น
2) ข้อมูลติดต่อ	(โปรดระบุ) เช่น เบอร์โทรศัพท์ ที่อยู่อีเมล ที่อยู่ตามทะเบียนบ้าน เป็นต้น
3) ข้อมูลทางการเงิน	(โปรดระบุ) เช่น เลขที่บัญชีธนาคาร
ข้อมูลอื่นๆ (ถ้ามี)	(โปรดระบุ)

ทั้งนี้ บริษัทไม่มีนโยบายจัดเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวของเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) ในกรณีที่บริษัทได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือ

(2) กรณีอื่นใดตามที่กฎหมายกำหนด

ข้อ 3. วัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

บริษัทดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน โดยมีวัตถุประสงค์ดังต่อไปนี้

วัตถุประสงค์	รายละเอียด	ฐานการประมวลผลข้อมูล
1. เพื่อการปฏิบัติตามสัญญาว่าจ้าง	เพื่อดำเนินการตามวัตถุประสงค์ตามสัญญาว่าจ้างในการจัดทำบัญชี หรือวัตถุประสงค์อื่น ๆ ในลักษณะเดียวกัน	ฐานการปฏิบัติตามสัญญา
2. (วัตถุประสงค์อื่นๆ โปรดระบุ)	รายละเอียด วัตถุประสงค์ โปรดระบุ	(ฐานกฎหมายตามมาตรา 24 หรือ 26 โปรดระบุ)

ในกรณีที่บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน เพื่อการปฏิบัติตามสัญญาหรือปฏิบัติตามกฎหมาย หากท่านไม่ให้ข้อมูลส่วนบุคคลนั้นแก่บริษัท บริษัทอาจจะไม่สามารถ

ปฏิบัติตามสัญญา หรือดำเนินการตามคำขอ เพื่อเข้าทำสัญญา หรือบริษัทอาจมีความรับผิดตามกฎหมาย หรืออาจมีผลกระทบอื่นใดที่เกี่ยวข้อง

ข้อ 4. การเปิดเผยข้อมูลส่วนบุคคลของท่าน

เพื่อดำเนินการตามวัตถุประสงค์ที่ระบุไว้ในประกาศความเป็นส่วนตัวฉบับนี้ ข้อมูลส่วนบุคคลของท่าน อาจมีการเปิดเผยหรือนำส่งให้กับหน่วยงานต่าง ๆ ภายในบริษัทและบุคคลหรือหน่วยงานภายนอก ดังนี้

4.1 หน่วยงานราชการ หน่วยงานกำกับดูแล หรือหน่วยงานอื่นตามที่กฎหมายกำหนด	ข้อมูลส่วนบุคคลของท่าน อาจมีการเปิดเผยหรือนำส่งให้กับองค์กรภายนอก ดังนี้ เช่น กรมสรรพากร สำนักงานประกันสังคม หรือหน่วยงานอื่นใดที่อาศัยอำนาจตามกฎหมาย เป็นต้น
4.2 องค์กรหรือบุคคลภายนอก	บริษัทอาจเปิดเผยข้อมูลของท่าน ให้กับองค์กรหรือบุคคลภายนอกที่มีการติดต่อสอบถามเพื่อวัตถุประสงค์ในการตรวจสอบการทำธุรกรรมต่าง ๆ ของท่าน เช่น สถาบันการเงิน หรือหน่วยงานภาครัฐ เป็นต้น
4.3 บุคคลหรือหน่วยงานอื่นที่เปิดเผยไป โปรดระบุ (ถ้ามี)	รายละเอียด โปรดระบุ

ข้อ 5. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

5.1 กรณีที่มีเหตุจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศ บริษัทจะปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและใช้มาตรการที่เหมาะสมเพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลของท่านจะได้รับความคุ้มครองและท่านสามารถใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่านได้ตามที่กฎหมายกำหนด รวมถึงบริษัทจะกำหนดให้ผู้ที่ได้รับข้อมูลส่วนบุคคลของท่านมีมาตรการปกป้องข้อมูลของท่านอย่างเหมาะสม และประมวลผลข้อมูลส่วนบุคคลดังกล่าวเท่าที่จำเป็นเท่านั้น และดำเนินการเพื่อป้องกันไม่ให้บุคคลอื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยมิชอบ

ข้อ 6. การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลของท่าน

6.1 บริษัทจะจัดเก็บข้อมูลส่วนบุคคลของท่านนานตราบเท่าที่จำเป็น โดยคำนึงถึงความจำเป็นและวัตถุประสงค์ที่บริษัทจะต้องเก็บรวบรวม ใช้และประมวลผล ซึ่งรวมถึงการปฏิบัติตามข้อกำหนดของกฎหมายที่ใช้บังคับ (โปรดระบุระยะเวลา หากมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่ชัดเจน

เช่น เก็บรักษาเป็นระยะเวลา 10 ปี นับแต่วันที่สิ้นสุดสัญญาเพื่อประโยชน์เรื่องอายุความในการเรียกร้อง เป็นต้น)

6.2 บริษัทจะยังดำเนินการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของท่านต่อไป แม้ว่าท่านจะยุติความสัมพันธ์กับบริษัท เท่าที่จำเป็นตามข้อกำหนดของกฎหมายเพื่อประโยชน์โดยชอบด้วยกฎหมาย หรือทำการเก็บในรูปแบบที่ทำให้ระบุตัวบุคคลไม่ได้ไม่ว่าทางตรงหรือทางอ้อม เช่น “การทำข้อมูลนิรนาม” (Anonymous Data) หรือ “การทำข้อมูลแฝงที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค” (Pseudonymous Data)

6.3 บริษัทจะดำเนินการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ทำให้ไม่สามารถระบุชื่อเจ้าของข้อมูลส่วนบุคคลได้เป็นการถาวร หรือโดยประการอื่นเพื่อจำกัดข้อมูลส่วนบุคคลทั้งหมดเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือเมื่อบริษัทต้องปฏิบัติตามคำขอของท่านให้บริษัททำการลบข้อมูลส่วนบุคคลของท่าน

ข้อ 7. บริษัทคุ้มครองข้อมูลส่วนบุคคลของท่านอย่างไร

บริษัทให้ความสำคัญด้านความปลอดภัยของข้อมูลส่วนบุคคลของท่านเป็นอันดับแรก เช่น การเข้ารหัส การจำกัดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล เพื่อให้ท่านมั่นใจว่าบุคลากรของบริษัทและบุคคลภายนอกที่ดำเนินการในนามของบริษัทได้ปฏิบัติตามมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งรวมถึงหน้าที่ในการป้องกันการรั่วไหลของข้อมูลและบริษัทใช้มาตรการรักษาความปลอดภัยที่เหมาะสมกับการประมวลผลข้อมูล

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้เป็นอย่างดีตามมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อรักษาความปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล โดยบริษัทได้กำหนดนโยบาย ระเบียบ และหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมาตรการเพื่อป้องกันไม่ให้ผู้รับข้อมูลไปจากบริษัทใช้ หรือเปิดเผยข้อมูลนอกวัตถุประสงค์ หรือโดยไม่มีอำนาจหรือโดยมิชอบ และบริษัทได้มีการปรับปรุงนโยบาย ระเบียบและหลักเกณฑ์ดังกล่าวเป็นระยะตามความจำเป็น และเหมาะสม นอกจากนี้ผู้บริหาร พนักงาน ผู้รับจ้าง ตัวแทน ที่ปรึกษา และผู้รับข้อมูลจากบริษัทมีหน้าที่ต้องรักษาความลับของข้อมูลส่วนบุคคลตามมาตรการรักษาความลับที่บริษัทกำหนด

ข้อ 8. สิทธิของเจ้าของข้อมูล

ท่านในฐานะเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการดำเนินการ ดังต่อไปนี้

(1) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)

ท่านมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมกับเราได้ ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของท่านอยู่กับเรา ซึ่งการถอนความยินยอมนี้จะไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมไปแล้ว

ทั้งนี้ การถอนความยินยอมของท่าน อาจส่งผลกระทบต่อการพิจารณางาน สิทธิประโยชน์ต่างๆ ที่ท่านพึงได้จากบริษัท หรือไม่ได้รับข้อมูลข่าวสารอันเป็นประโยชน์แก่ท่าน เป็นต้น เพื่อประโยชน์ของท่าน จึงควรศึกษาและสอบถามถึงผลกระทบก่อนเพิกถอนความยินยอม

(2) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access)

ท่านมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของท่านและขอให้เราทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้แก่ท่าน รวมถึงขอให้เราเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ท่านไม่ได้ให้ความยินยอมต่อเราได้

(3) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification)

ท่านมีสิทธิในการขอให้เราแก้ไขข้อมูลที่ไม่ถูกต้อง หรือ เพิ่มเติมข้อมูลที่ไม่สมบูรณ์

(4) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure)

ท่านมีสิทธิในการขอให้เราทำการลบข้อมูลของท่านด้วยเหตุบางประการได้

(5) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restriction of processing)

ท่านมีสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

(6) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability)

ท่านมีสิทธิในการโอนย้ายข้อมูลส่วนบุคคลของท่านที่ท่านให้ไว้กับเราไปยังผู้ควบคุมข้อมูลรายอื่น หรือตัวท่านเองด้วยเหตุบางประการได้

(7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object)

ท่านมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของท่านด้วยเหตุบางประการได้

(8) สิทธิในการร้องเรียน (right to complaint)

ท่านมีสิทธิในการร้องเรียนต่อต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับการแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามระเบียบและวิธีการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด หากท่านเล็งเห็นว่าบริษัทดำเนินการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล เมื่อบริษัทได้รับคำร้องขอดังกล่าวแล้ว จะดำเนินการภายในระยะเวลาที่กฎหมายกำหนด อนึ่ง บริษัทขอสงวนสิทธิ์ที่จะปฏิเสธหรือไม่ดำเนินการตามคำร้องขอดังกล่าวในกรณีที่กฎหมายกำหนด

ข้อ 9. ช่องทางการติดต่อ

หากท่านมีข้อสงสัย หรือต้องการสอบถามข้อมูลเกี่ยวกับ การเก็บรวบรวม ใช้ และ/หรือ เปิดเผย การใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน ตามประกาศความเป็นส่วนตัวฉบับนี้ ท่านสามารถติดต่อได้ตามรายละเอียดที่ปรากฏดังต่อไปนี้

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ชื่อ.....

ที่อยู่.....

อีเมล.....

โทรศัพท์.....

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) (ถ้ามี)

ชื่อ : .....

อีเมล : .....

โทรศัพท์ : .....

5.3 หนังสือขอความยินยอม (Consent Form)

ตัวอย่าง หนังสือขอความยินยอมเกี่ยวกับข้อมูลส่วนบุคคล

เพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 **บริษัท สอบบัญชี จำกัด** (“**บริษัท**”) ซึ่งจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูล เพื่อปฏิบัติตามภาระหน้าที่ของบริษัทที่มีตามกฎหมายหรือตามสัญญาที่มีอยู่กับเจ้าของข้อมูลหรือเพื่อประโยชน์อันชอบด้วยกฎหมายของบริษัท โดยบริษัทได้ระบุรายละเอียดและขอบเขตการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล เช่น วัตถุประสงค์ของการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ ระยะเวลาในการจัดเก็บ บุคคลหรือนิติบุคคลที่บริษัทอาจเปิดเผยข้อมูลส่วนบุคคลให้ สิทธิอันชอบด้วยกฎหมายของบริษัทในการจัดเก็บข้อมูล สิทธิของเจ้าของข้อมูลตามกฎหมาย เป็นต้น ตามที่ปรากฏในประกาศความเป็นส่วนตัว

ข้าพเจ้านาย/นาง/นางสาว..... นามสกุล…….....……..... บัตรประจำตัวประชาชนเลขที่.....

☐ **ยินยอม** ☐ **ไม่ยินยอม** ให้บริษัทเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของข้าพเจ้า ได้แก่ ..... (ระบุข้อมูลที่จัดเก็บรวบรวม) เพื่อ..... (ระบุวัตถุประสงค์ในการนำข้อมูลมาประมวลผล)

ทั้งนี้ ก่อนการแสดงเจตนา ข้าพเจ้าได้อ่านหนังสือยินยอมเกี่ยวกับข้อมูลส่วนบุคคลฉบับนี้โดยตลอดแล้ว ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจ ปราศจากการบังคับหรือชักจูง และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้ เว้นแต่ในกรณีมีข้อจำกัดสิทธิตามกฎหมายหรือยังมีสัญญาระหว่างข้าพเจ้ากับบริษัทที่ให้ประโยชน์แก่ข้าพเจ้าอยู่

กรณีที่ข้าพเจ้าประสงค์จะขอถอนความยินยอม ข้าพเจ้าทราบว่าการถอนความยินยอมจะมีผลทำให้ข้าพเจ้าได้รับความสะดวกในการใช้บริการน้อยลง หรือไม่สามารถเข้าถึงฟังก์ชันการใช้งานบางอย่างได้ ทั้งนี้ ข้าพเจ้าทราบว่าการถอนความยินยอมดังกล่าว ไม่มีผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม

ในกรณีที่ท่านประสงค์ร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดไว้ ท่านสามารถติดต่อบริษัท เพื่อร้องขอใช้สิทธิตามกฎหมายผ่านช่องทาง [โปรดระบุช่องทางการติดต่อกับสำนักงานผู้ควบคุมข้อมูล เช่น ทางอีเมล]

ท่านสามารถอ่านรายละเอียดเกี่ยวกับประกาศความเป็นส่วนตัวสำหรับลูกค้าได้ตามเอกสารแนบท้าย เว็บไซต์ของบริษัท (link……) หรือ แสกน QR Code

ลงชื่อ…….....

(.....)

วันที่.....

5.4 แบบคำขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request)

ตัวอย่าง แบบคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

วันที่ .....

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการขอใช้สิทธิดำเนินการต่อข้อมูลส่วนบุคคลของตนซึ่งอยู่ในความดูแลของ บริษัท สอบบัญชี จำกัด (“บริษัท”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล โดยท่านสามารถใช้สิทธิดังกล่าวได้โดยการกรอกรายละเอียดในแบบคำขอนี้ และยื่นคำขอนี้ด้วยตนเองแก่บริษัทผ่านช่องทาง จดหมายอิเล็กทรอนิกส์ (E-Mail) (ระบุช่องทางอื่น หากมี)

☐ ผู้ยื่นคำขอเป็นเจ้าของข้อมูลส่วนบุคคล

☐ ยื่นคำขอเป็นผู้แทนของเจ้าของข้อมูลส่วนบุคคล (โปรดระบุรายละเอียดของเจ้าของข้อมูลส่วนบุคคล)

<u>รายละเอียดของเจ้าของข้อมูลส่วนบุคคล</u>

ชื่อ – นามสกุล.....

เลขบัตรประจำตัวประชาชน/ เลขหนังสือเดินทาง.....

เบอร์โทรศัพท์ติดต่อ.....

อีเมล.....

<u>เอกสารประกอบการขอใช้สิทธิ</u>

เอกสารเพื่อการยืนยันตัวตนของผู้ยื่นคำขอ

☐ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย)

☐ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญชาติไทย)

เอกสารประกอบการดำเนินการแทน (เฉพาะกรณียื่นคำขอแทนเจ้าของข้อมูลส่วนบุคคล)

☐ หนังสือมอบอำนาจ

<u>โปรดระบุสถานะความสัมพันธ์ของท่านที่มีต่อบริษัท</u>

☐ ลูกค้า

☐ เจ้าหน้าที่ ผู้ปฏิบัติงาน พนักงาน

☐ ผู้สมัครงาน

☐ คู่สัญญา

☐ อื่น ๆ (โปรดระบุ) .....

<u>โปรดระบุสิทธิที่ท่านประสงค์จะดำเนินการ</u>

☐ เพิกถอนความยินยอม

☐ ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคล รวมถึงขอให้บริษัทเปิดเผยที่มาของข้อมูลส่วนบุคคลที่ท่านไม่ได้ให้ความยินยอมในการเก็บรวบรวม

☐ ขอแก้ไขข้อมูลส่วนบุคคล

☐ ขอให้ลบข้อมูลส่วนบุคคล

☐ ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล

☐ ขอระงับการประมวลผลข้อมูลส่วนบุคคล

☐ ขอให้บริษัทโอนย้ายข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น

โปรดระบุวัตถุประสงค์และเหตุผลประกอบคำขอของท่าน

……..……..……..……..……..……..……..……

……..……..……..……..……..……..……..……

……..……..……..……..……..……..……..……

……..……..……..……..……..……..……..……..

<u>หมายเหตุ</u>

บริษัทจะดำเนินการตามคำขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำขอพร้อมเหตุผลและข้อมูลประกอบคำขอต่าง ๆ รวมถึงเอกสารหลักฐานประกอบจากท่านครบถ้วน ทั้งนี้ ขอสงวนสิทธิ์ในการขยายเวลาดังกล่าวออกไป หากบริษัทได้รับข้อมูลไม่เพียงพอในการประกอบการดำเนินการ

ในกรณีที่ บริษัทมีความจำเป็นต้องปฏิเสธคำขอใช้สิทธิของท่าน บริษัทจะแจ้งเหตุผลการปฏิเสธแก่ท่านทราบทางอีเมล (สำนักงานสามารถระบุช่องทางการแจ้งเหตุปฏิเสธ)

ผู้ยื่นคำขอได้อ่านและเข้าใจเนื้อหาของแบบคำขอฉบับนี้แล้ว และยืนยันว่าข้อมูลที่ได้แจ้งแก่บริษัทมีความถูกต้อง ครบถ้วน สมบูรณ์ทุกประการ รวมทั้งขอยืนยันและรับประกันว่าผู้ยื่นคำขอมีสิทธิอย่างถูกต้องตามกฎหมาย จึงได้ลงลายมือชื่อตามที่ระบุข้างล่างนี้

..... ผู้ยื่นคำขอ

(.....)

5.5 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

ตัวอย่าง บันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

(Data Processing Agreement)

บันทึกข้อตกลงแนบท้ายสัญญา..... (ระบุสัญญาหลัก)

บันทึกข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (“**บันทึกข้อตกลง**”) ฉบับนี้ทำขึ้น เมื่อวันที่ ..... ณ ..... ระหว่าง

บริษัท สอบบัญชี จำกัด โดย**.....** (ระบุชื่อ-นามสกุลของกรรมการผู้มีอำนาจ) กรรมการผู้มีอำนาจ สำนักงานแห่งใหญ่ตั้งอยู่ที่เลขที่ ..... ซึ่งต่อไปนี้ เรียกว่า “บริษัท” หรือ“ผู้ควบคุมข้อมูลส่วนบุคคล” ฝ่ายหนึ่ง กับ

บริษัท.....โดย..... กรรมการผู้มีอำนาจ สำนักงานตั้งอยู่ที่ .....อีเมลติดต่อทางธุรกิจ .....หมายเลขโทรศัพท์ติดต่อ ..... ซึ่งต่อไปในบันทึกข้อตกลงฉบับนี้ เรียกว่า **“ผู้ให้บริการ”** หรือ **“ผู้ประมวลผลข้อมูลส่วนบุคคล”** อีกฝ่ายหนึ่ง

บริษัทและผู้ให้บริการได้เข้าทำสัญญา..... ลงวันที่ ..... โดยมีวัตถุประสงค์ในการ.....(ระบุวัตถุประสงค์ตามสัญญาหลัก) ซึ่งในการดำเนินการตามสัญญาดังกล่าว (ซึ่งต่อไปในบันทึกข้อตกลงฉบับนี้จะเรียกว่า “**สัญญาหลัก**”) บริษัทมีความจำเป็นที่จะต้องเปิดเผยข้อมูลส่วนบุคคลของลูกค้าให้แก่ผู้ให้บริการ และผู้ให้บริการอาจเข้าถึง ได้รับ และ/หรือ เก็บรวบรวม ใช้ เปิดเผย (“**ประมวลผล**”) ข้อมูลส่วนบุคคลดังกล่าวตามคำสั่งหรือในนามของบริษัทเพื่อการให้บริการเพื่อให้เป็นไปตามสัญญาที่มีอยู่

ดังนั้น คู่สัญญาทั้งสองฝ่ายจึงตกลงกันดังนี้

ข้อ 1. คำรับรองของคู่สัญญา

1.1 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ตกลงเปิดเผยหรือให้ผู้ให้บริการเข้าถึงข้อมูลส่วนบุคคลเพื่อบรรลุวัตถุประสงค์ในการดำเนินการตามคำสั่งหรือในนามของบริษัทเท่านั้น โดยที่ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตกลงที่จะดำเนินการภายใต้คำสั่งหรือในนามของ ผู้ควบคุมข้อมูลส่วนบุคคลตามที่กำหนดในสัญญาหลักที่มีอยู่ รวมถึงบันทึกข้อตกลงฉบับนี้เท่านั้น

1.2 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า รายละเอียดการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามวัตถุประสงค์ ดังต่อไปนี้

(1) ..... (ระบุวัตถุประสงค์)

(2) ..... (ระบุวัตถุประสงค์)

นอกเหนือจากวัตถุประสงค์ที่กล่าวมาในวรรคก่อน ถือว่าเป็นการกระทำหรือการประมวลผลข้อมูลส่วนบุคคลของผู้ให้บริการโดยลำพัง ไม่เกี่ยวข้องกับบริษัทในทางใด ๆ และผู้ให้บริการจะรับผิดเกี่ยวกับการดำเนินการดังกล่าวแต่เพียงผู้เดียวเสมือนหนึ่งว่าผู้ให้บริการเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของงานดังกล่าวเป็นการส่วนตัว

1.3 ผู้ให้บริการรับรองว่า จะจัดให้มีมาตรการรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคลที่ได้รับมอบ และจะจัดให้มีการดูแลรักษามาตรการดังกล่าวเป็นครั้งคราว ตามที่บริษัทเห็นสมควร

1.4 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า บันทึกข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาหลักที่มีอยู่ เว้นแต่จะกำหนดไว้เป็นอย่างอื่นในบันทึกข้อตกลงฉบับนี้ ทั้งนี้ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อกำหนดของสัญญาหลักที่มีอยู่ ยังคงไม่เปลี่ยนแปลงและมีผลใช้บังคับอย่างสมบูรณ์

ข้อ 2. ข้อตกลงและเงื่อนไข

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อกำหนดและเงื่อนไขต่อไปนี้ใช้บังคับเกี่ยวกับข้อมูลส่วนบุคคล

2.1 ข้อกำหนดทั่วไป

คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมให้ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้น ผู้ให้บริการจึงตกลงที่จะปฏิบัติตามคำสั่งเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัทอย่างเคร่งครัด และจะไม่กระทำการใด ๆ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในนามของบริษัทโดยไม่ได้รับอนุญาตเป็นหนังสือ และผู้ให้บริการจะปฏิบัติการอื่นใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

2.2 ข้อมูลส่วนบุคคลที่เปิดเผย ผู้ควบคุมข้อมูลส่วนบุคคลตกลงแบ่งปันข้อมูลส่วนบุคคลดังรายการต่อไปนี้แก่ผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้

ข้อมูลส่วนบุคคลที่แบ่งปันโดยผู้ควบคุมข้อมูลส่วนบุคคล	วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล
1. .....(ระบุข้อมูลส่วนบุคคลที่แบ่งปันโดยผู้ควบคุมข้อมูลส่วนบุคคล)	1. เพื่อความจำเป็นในการ ... (ระบุเหตุผลความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคล ระหว่างคู่สัญญา เช่น เพื่อปฏิบัติตามสัญญาว่าจ้างในการจัดทำเงินเดือน)
2.	2..... .....
3.	3..... .....

2.3 การประมวลผลข้อมูลส่วนบุคคล

ในการประมวลผลข้อมูลส่วนบุคคล ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องปฏิบัติ ดังนี้

(1) ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงแต่ไม่จำกัดเพียง นโยบายคุ้มครองข้อมูลส่วนบุคคล ประกาศความเป็นส่วนตัว ข้อตกลงหรือแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในการให้บริการและการปฏิบัติตามหน้าที่อื่น ๆ ของตนภายใต้สัญญาที่มีอยู่ทั้งหมด

(2) แจ้งให้พนักงาน ตัวแทน บุคลากรของตนทราบและดำเนินการให้แน่ใจว่าบุคคลเหล่านั้นปฏิบัติตามคำสั่งของบริษัท และกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งหมดเท่านั้น

(3) การประมวลผลข้อมูลส่วนบุคคลต้องทำภายใต้คำสั่งที่เป็นลายลักษณ์อักษรหรือมีบันทึกจากบริษัท เว้นแต่กรณีที่ผู้ให้บริการจะต้องปฏิบัติตามกฎหมาย

(4) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทั้งปวงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามสมควร

(5) แจ้งให้บริษัททราบเป็นหนังสือทันทีโดยไม่ชักช้า เมื่อผู้ให้บริการทราบถึงกรณี ดังต่อไปนี้

• การฝ่าฝืนอย่างร้ายแรงในการรักษาความปลอดภัยหรือมีเหตุที่น่าจะเชื่อได้ว่าข้อมูลส่วนบุคคลอาจถูกเปิดเผย เข้าถึง หรือใช้โดยไม่ได้รับอนุญาต รวมถึงมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

• เมื่อมีคำร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

• เมื่อมีหมายเรียก หรือคำสั่งจากศาล หรือเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐผู้มีอำนาจ หรือหน่วยงานกำกับดูแล เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

(6) ดำเนินการตามที่เหมาะสมและสมควร โดยค่าใช้จ่ายของผู้ให้บริการ รวมไปถึงแต่ไม่จำกัดเพียงการแจ้งบุคคลที่ได้รับผลกระทบ การเยียวยาผลกระทบ จากการที่ผู้ให้บริการไม่สามารถดำเนินการรักษาความปลอดภัยหรือป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตต่อข้อมูลส่วนบุคคลได้ และ

(7) ไม่โอนข้อมูลส่วนบุคคลออกจาก หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากบุคคลอื่นที่อยู่นอกประเทศไทยโดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากบริษัทก่อน

2.4 การป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้ให้บริการรับรองและรับประกันว่า ณ วันที่ตกลงให้มีผลใช้บังคับและตลอดระยะเวลาของสัญญาที่มีอยู่ผู้ให้บริการได้จัดให้มีและจะจัดให้มีการควบคุมเมื่อมีการลงข้อมูล การเข้าถึง การแทรกแซง การเปิดเผย การใส่รหัสและมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้มาตรฐานสากลและเพียงพอเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะปลอดภัยและคงไว้ซึ่งความลับ ซึ่งรวมถึง การได้รับการป้องกันจากการคุกคามหรือภยันตรายที่อาจมีขึ้นต่อความสมบูรณ์ของการเข้าถึงหรือใช้โดยไม่ได้รับอนุญาตซึ่งข้อมูลส่วนบุคคล

2.5 เหตุการละเมิดข้อมูลส่วนบุคคล

ในกรณีที่เกิดเหตุการละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเกิดกับบริษัท และ/หรือผู้ให้บริการ และ/หรือผู้ให้บริการช่วง คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่าจะดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด แจ้งให้คู่สัญญาอีกฝ่ายรับทราบในทันทีโดยไม่ชักช้า ภายในกำหนด 48 (สี่สิบแปด) ชั่วโมงนับแต่ทราบเหตุ บรรเทาความเสียหาย รวมไปถึงแต่ไม่จำกัดเพียงให้ความช่วยเหลือ อำนวยความสะดวกซึ่งกันและกัน

ข้อ 3. หน้าที่ของบริษัท

บริษัทตกลงจะดำเนินการ ดังต่อไปนี้

3.1 บริษัทเป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามบันทึกข้อตกลงฉบับนี้

3.2 บริษัทตกลงจะจัดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อทำให้มั่นใจว่าข้อมูลส่วนบุคคลมีการประมวลผลเท่าที่จำเป็น รวมถึงจำนวนข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ขอบเขต ระยะเวลาการเก็บรักษา และการเข้าถึงข้อมูล โดยมาตรการดังกล่าวจะต้องทำให้มั่นใจได้ว่าข้อมูลส่วนบุคคลจะถูกจำกัดไม่ให้มีการถูกแทรกแซงโดยบุคคลอื่น

ข้อ 4. หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงจะดำเนินการ ดังต่อไปนี้

4.1 ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ตลอดจนปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

4.2 ประมวลผลข้อมูลส่วนบุคคลตามที่บริษัทกำหนดไว้เป็นลายลักษณ์อักษรเท่านั้น

4.3 ทำให้มั่นใจว่าบุคคลที่ได้รับอนุญาตในการประมวลผลข้อมูลส่วนบุคคลจะเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นความลับหรือดำเนินการตามกฎหมายอย่างเหมาะสม

4.4 ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) เพื่อทำให้มั่นใจว่าระดับความมั่นคงปลอดภัยเป็นไปอย่างเหมาะสมตามความเสี่ยงที่อาจเกิดต่อสิทธิและเสรีภาพของบุคคล และมาตรการดังกล่าวนี้ได้สอดคล้องกับมาตรา 40 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

4.5 ผู้ประมวลผลข้อมูลส่วนบุคคลจะเก็บรักษาและไม่เปิดเผยข้อมูลส่วนบุคคลของบริษัทต่อบุคคลภายนอก เว้นแต่จะได้รับความยินยอมเป็นหนังสือล่วงหน้าจากบริษัท

4.6 ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งให้บริษัททราบทันทีเมื่อเกิดเหตุการณ์รั่วไหล การละเมิด การเข้าถึง ใช้ หรือเปลี่ยนแปลงข้อมูลส่วนบุคคลที่ได้รับจากบริษัทโดยไม่ได้รับอนุญาต

4.7 เมื่อบริษัทเห็นสมควร ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการลบหรือส่งคืนข้อมูลส่วนบุคคลให้แก่บริษัททั้งหมดภายหลังจากการประมวลผลข้อมูลส่วนบุคคลสิ้นสุด รวมถึงการลบสำเนาข้อมูลที่มีอยู่ทั้งหมด เว้นแต่จะมีกฎหมายกำหนดให้เก็บข้อมูลส่วนบุคคลนั้นต่อไปได้

4.8 เมื่อบริษัทร้องขอ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดเตรียมข้อมูลที่จำเป็นเพื่อให้บริษัทตรวจสอบถึงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้บริษัทหรือผู้มีอำนาจของบริษัทสามารถดำเนินการตรวจสอบการปฏิบัติงานได้

4.9 ปกป้องและชดใช้ความสูญเสีย ความเสียหาย และค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นต่อบริษัทอันเป็นผลมาจากการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือการกระทำผิดข้อใดข้อหนึ่งในบันทึกข้อตกลงฉบับนี้ของผู้ประมวลข้อมูลส่วนบุคคล

ข้อ 5. การใช้หรือจ้างช่วงประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่ใช้ หรือจ้างช่วงผู้ประมวลผลข้อมูลส่วนบุคคลอื่นโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรล่วงหน้าจากผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีสัญญาที่กำหนดให้ผู้รับช่วงผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย เช่นเดียวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามบันทึกข้อตกลงฉบับนี้ นอกจากนี้ผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลต้องรับประกันว่าจะใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามกฎหมายและมาตรการต้องให้ความคุ้มครองในระดับเดียวกับมาตรการที่ระบุตามบันทึกข้อตกลงฉบับนี้

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบความเสียหายต่อว่าผู้ควบคุมข้อมูลส่วนบุคคลเมื่อผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อ 6. การแจ้งเตือนหากเกิดปัญหาด้านความปลอดภัย

6.1 กรณีมีการละเมิดต่อมาตรการรักษาความปลอดภัย ผู้ให้บริการมีหน้าที่ทำการประเมินและตอบสนองต่อการกระทำใด ๆ ซึ่งอาจมีลักษณะเป็นการ เข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ทั้งนี้ บุคลากรของผู้ให้บริการตลอดจน บริษัทในเครือของผู้ให้บริการถูกกำหนดให้มีหน้าที่ที่จะตอบสนองต่อเหตุการณ์ข้างต้น

6.2 กระบวนการแจ้งเตือน ในกรณีที่ผู้ให้บริการตระหนักได้ว่ามีการกระทำอันเป็นการละเมิดต่อความปลอดภัยซึ่ง ก่อให้เกิดความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคล โดยไม่ชอบด้วยกฎหมาย ผู้ให้บริการจะทำการแจ้งต่อผู้ใช้บริการโดยไม่ชักช้า ทั้งนี้ภายในระยะเวลา 48 (สี่สิบแปด) ชั่วโมง นับแต่ทราบเหตุ

6.3 การดำเนินการ ผู้ให้บริการจะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกัน ปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ผู้ใช้บริการภายใต้ขอบเขตที่กฎหมายกำหนดดังต่อไปนี้

- รายละเอียดของลักษณะและผลที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ถูกละเมิด (หากเป็นไปได้) และ
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการละเมิด

ข้อ 7. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อผู้ให้บริการหรือผู้ให้บริการช่วง แล้วแต่กรณี เพื่อขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ให้บริการตกลงที่จะแจ้งบริษัท ทันทีโดยไม่ชักช้า หรือผู้ให้บริการอาจดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ก็ต่อเมื่อผู้ให้บริการไม่สามารถติดต่อบริษัท และต้องดำเนินการข้างต้นโดยไม่อาจหลีกเลี่ยงได้ ทั้งนี้ ผู้ให้บริการต้องพิจารณาถึงปัจจัยต่าง ๆ โอกาสที่จะเกิดความเสียหายแก่บริษัท แนวทางปฏิบัติระหว่างคู่สัญญาทั้งสองฝ่าย โดยมีบันทึกการพิจารณาดังกล่าวเป็นหลักฐานแล้วดำเนินการข้างต้น อนึ่ง บันทึกข้างต้นไม่ตัดสิทธิบริษัทที่จะเรียกร้องค่าเสียหายกับผู้ให้บริการ (ถ้ามี)

ข้อ 9. ความสมบูรณ์ของสัญญา

ในกรณีที่ข้อตกลงใด ข้อตกลงหนึ่ง ภายใต้บันทึกข้อตกลงนี้ เป็นโมฆะ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่า ข้อตกลงอื่นภายใต้บันทึกข้อตกลงนี้ที่ไม่เป็นโมฆะ มีผลบังคับใช้ระหว่างคู่สัญญาทั้งสองฝ่ายต่อไป และคู่สัญญาทั้งสองฝ่ายจะร่วมกันแก้ไขข้อตกลงที่มีผลเป็นโมฆะให้มีผลบังคับใช้ได้ตามกฎหมาย โดยให้มีผลในทางการค้าที่ใกล้เคียงกับข้อตกลงที่มีผลเป็นโมฆะนั้นมากที่สุดเท่าที่จะทำได้

ข้อ 10. การแก้ไขเปลี่ยนแปลง

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ ไม่สามารถดำเนินการแก้ไข เปลี่ยนแปลงข้อตกลงได้ เว้นแต่จะทำขึ้นเป็นหนังสือและลงนามโดยคู่สัญญาทั้งสองฝ่ายหรือโดยการบอกกล่าวล่วงหน้าจากบริษัทโดยให้การเปลี่ยนแปลงดังกล่าวมีผลบังคับใช้ไม่เกิน ..... วัน (โปรดระบุจำนวนวัน) นับแต่วันที่บริษัทได้ส่งคำบอกกล่าวข้างต้น

ข้อ 11. ความรับผิดตามสัญญา

ผู้ให้บริการจะรับผิดชอบชดใช้ให้กับบริษัทสำหรับค่าปรับ ความสูญเสีย หรือความเสียหายทั้งหมด อันเนื่องมาจากการที่ผู้ให้บริการฝ่าฝืนข้อกำหนดหรือเงื่อนไขใดๆ ภายใต้บันทึกข้อตกลงนี้

ข้อ 10. ความสิ้นสุดของสัญญา

10.1 บันทึกข้อตกลงฉบับนี้อาจสิ้นสุดได้โดยการตกลงร่วมกันระหว่างคู่สัญญาทั้งสองฝ่าย หรือการบอกกล่าวเป็นหนังสือล่วงหน้า ไม่เกิน ..... วัน (ระบุจำนวนวัน) นับแต่วันที่คู่สัญญาฝ่ายหนึ่งได้ส่งคำบอกกล่าวข้างต้น หรือสิ้นสุดตามการสิ้นสุดของสัญญาหลักที่ได้อ้างถึงบันทึกข้อตกลงฉบับนี้

10.2 บันทึกข้อตกลงฉบับนี้ เป็นสัญญาอุปกรณ์ของสัญญาหลัก หากสัญญา.....(ระบุชื่อสัญญาหลัก) สิ้นผลผูกพันลงไม่ว่ากรณีใด ให้ถือว่าบันทึกข้อตกลงฉบับนี้สิ้นผลตามกฎหมายด้วยโดยปริยาย

เพื่อเป็นหลักฐานแห่งการนี้คู่สัญญาทั้งสองฝ่ายภายใต้บันทึกข้อตกลงฉบับนี้ ได้รับทราบและเข้าใจ คำรับรอง ข้อตกลงและเงื่อนไข ตลอดจนเอกสารแนบท้ายที่ได้ตกลงกันไว้ทั้งหมดแล้ว และได้ลง

ลายมือชื่อพร้อมประทับตราสำคัญ (หากมี) ในต้นฉบับบันทึกข้อตกลงนี้ จำนวนสองฉบับ โดยต่างฝ่ายต่างถือต้นฉบับไว้ฝ่ายละฉบับเพื่อเก็บไว้เป็นหลักฐาน

ลงชื่อ……..…….....……ผู้ควบคุมข้อมูล
(……)
กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ
บริษัท สอบบัญชี จำกัด

ลงชื่อ……..…….....……ผู้ให้บริการ
(……)
กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ
บริษัท……

ลงชื่อ.....พยาน
(.....)

ลงชื่อ.....พยาน
(.....)

5.6 หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Notifications)

1) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อมีการประเมินระดับความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเรียบร้อยแล้ว และพบว่าต้องมีการตัดสินใจที่จะแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 37 (4) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่มีเหตุผลที่ถูกต้องตามกฎหมายที่ทำให้ไม่สามารถแจ้งเหตุรั่วไหลของข้อมูลส่วนบุคคลได้ในระยะเวลาที่กำหนด

ทั้งนี้ การแจ้งเหตุละเมิดที่มีความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งจะต้องแจ้งให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ จะต้องมีรายละเอียดตามตัวอย่าง ดังต่อไปนี้

ตัวอย่าง

หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

บริษัท สอบบัญชี จำกัด

วันที่ .....

เรียน สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ตามที่ บริษัท สอบบัญชี จำกัด (“บริษัท”) ได้ตรวจพบเหตุการละเมิดข้อมูลส่วนบุคคลที่บริษัทเก็บรักษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล นั้นบริษัทได้พิจารณาแล้วเห็นว่าเหตุการณ์ละเมิดดังกล่าวมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

ในการนี้ เพื่อเป็นการปฏิบัติตามความของมาตรา 37(4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัท จึงขอนำเรียนให้ทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล	ระบุรายละเอียดเหตุการณ์ที่เป็นภัยคุกคามข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะละเมิดสิทธิเสรีภาพของบุคคล เช่น 1. ข้อมูลถูกลักลอบคัดลอกออกไปภายนอกโดยอดีตพนักงาน 2. ฐานข้อมูลขององค์กรถูกโจมตีและเข้าถึงโดยมิชอบ 3. ฐานข้อมูลขององค์กรถูกโจมตีโดย Ransomware ทำให้ไม่สามารถให้บริการลูกค้า ได้ในช่วงระยะเวลาหนึ่ง หรือ ทำให้บริการเกิดล่าช้า 4. เอกสาร (กระดาษ) ที่มีรายการข้อมูลส่วนบุคคลถูกโจรกรรม

วันเวลาที่ทราบเหตุ	ระบุวันเวลาที่ทราบเหตุ
ผู้ที่รายงานเหตุให้ทราบ (หากมี)	ระบุชื่อผู้ที่แจ้ง/พบเหตุการณ์ เป็นคนแรก
รายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ระบุรายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการณ์ เช่น ชื่อ-นามสกุล อีเมล ประวัติสุขภาพ
รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคล	ระบุรูปแบบผลกระทบที่เกิดกับข้อมูลส่วนบุคคล เช่น • ถูกเปิดเผยต่อสาธารณะและอาจทำให้เจ้าของข้อมูลส่วนบุคคลเสื่อมเสีย • อาจถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต และนำไปใช้ประโยชน์โดยมิชอบ
รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคล	ระบุจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
มาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล	ระบุมาตรการ/การดำเนินการเพื่อหยุดยั้งเหตุภัยคุกคาม เช่น ระงับการใช้งานระบบทันที เป็นต้น
การแจ้งเหตุต่อเจ้าของ ข้อมูลส่วนบุคคล (เฉพาะกรณีมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของบุคคล)	ระบุการดำเนินการของบริษัท ในการแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล (หากมี) พร้อมมาตรการเยียวยา
ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ-นามสกุล……. สถานที่ติดต่อ: ……... ช่องทางการติดต่อ: ……...

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

……..……

(.....)

กรรมการผู้มีอำนาจลงนาม

2) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

บริษัทที่มีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่มีการประเมินความเสี่ยงการรั่วไหลของข้อมูลส่วนบุคคลและพบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล จะต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ

ตัวอย่าง

หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

บริษัท สอบบัญชี จำกัด

วันที่ ……..……...

เรียน ……..(เจ้าของข้อมูลส่วนบุคคล)

ตามที่ บริษัท สอบบัญชี จำกัด (“บริษัท”) ได้ตรวจพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่บริษัทเก็บรักษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคล นั้น บริษัทได้พิจารณาแล้วเห็นว่า เหตุการณ์ละเมิดดังกล่าวมีความเสี่ยงสูงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของท่าน

ในการนี้ เพื่อเป็นการปฏิบัติตามความของมาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัท จึงขอนำเรียนให้ท่านทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและจะดำเนินการเยียวยาแก่ท่านโดยเร็วที่สุดต่อไป โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล	ระบุรายละเอียดเหตุการณ์ที่เป็นภัยคุกคามข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะละเมิดสิทธิเสรีภาพของบุคคล เช่น 1. ข้อมูลถูกลักลอบคัดลอกออกไปภายนอกโดยอดีตพนักงาน 2. ฐานข้อมูลขององค์กรถูกโจมตีและเข้าถึงโดยมิชอบ 3. ฐานข้อมูลขององค์กรถูกโจมตีโดย Ransomware ทำให้ไม่สามารถให้บริการประชาชน/ลูกค้า ได้ในช่วงระยะเวลาหนึ่ง หรือ ทำให้บริการเกิดล่าช้า 4. เอกสาร (กระดาษ) ที่มีรายการข้อมูลส่วนบุคคลถูกโจรกรรม
วันเวลาที่ทราบเหตุ	ระบุวันเวลาที่ทราบเหตุ
รายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ระบุรายการข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุการณ์ เช่น ชื่อ-นามสกุล อีเมล ประวัติสุขภาพ

รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคล **รูปแบบผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคล**	ระบุรูปแบบผลกระทบที่เกิดกับข้อมูลส่วนบุคคล เช่น • ถูกเปิดเผยต่อสาธารณะและอาจทำให้เจ้าของข้อมูลส่วนบุคคลเสื่อมเสีย • ถูกลบทำลายโดยไม่ตั้งใจทำให้ประชาชน/ลูกค้า ไม่ได้รับความสะดวกในการใช้บริการ • อาจถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต และนำไปใช้ประโยชน์โดยมิชอบ
จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ระบุจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
มาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล	ระบุมาตรการ/การดำเนินการเพื่อหยุดยั้งเหตุภัยคุกคาม เช่น ระงับการใช้งานระบบทันที, เรียกคืน (Recall) อีเมลที่ส่งผิดพลาดทันที เป็นต้น
ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ชื่อ-นามสกุล..... สถานที่ติดต่อ: ..... ช่องทางการติดต่อ: .....

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

.....

(.....)

กรรมการผู้มีอำนาจลงนาม

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล.กรุงเทพฯ: นิติธรรม, 2564.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล.กฎหมายคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ: ศูนย์การพิมพ์แก่นจันทร์, 2563.พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. https://ratchakitcha.soc.go.th/documents/17082307.pdf

พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566

https://ratchakitcha.soc.go.th/documents/140A048N0000000004500.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. 2565.

https://www.mdes.go.th/uploads/tinymce/source/สคส/ระเบียบฯการยื่นการไม่รับเรื่องการยุติเรื่องการพิจารณาฯคำร้องเรียน2565.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565.

https://ratchakitcha.soc.go.th/documents/139D140S0000000002400.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกระบวนการการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000002600

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565.

https://ratchakitcha.soc.go.th/documents/139D140S0000000002800.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565.

https://ratchakitcha.soc.go.th/documents/139D140S0000000003200.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2566

https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf

DBC Group | PDPA THAILAND | dcti | pdpa dpo SERVICE

PDPA THAILAND

ให้คำปรึกษา พร้อมจัดทำ PDPA & DPO ครบวงจร โดยทีมผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

เมื่อความไม่รู้ ความไม่เข้าใจ PDPA อย่างแท้จริง
ทำให้เกิดความเสี่ยงที่จะทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ปิดจุดอ่อน แก้ไขข้อผิดพลาด ด้วยบริการของเรา

PDPA&DPO Consultant

ให้คำปรึกษาทางด้านกฎหมาย การบริหารจัดการ
กระบวนการการทำงาน และซอฟต์แวร์ที่เกี่ยวข้อง
กับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Auditor

ตรวจสอบเอกสาร กระบวนการการทำงาน
กระบวนการบริหารจัดการ และเทคโนโลยี
ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Tools

จัดหาเครื่องมือที่จำเป็นในการปฏิบัติตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
เช่น Consent, RoPA, DSRM และ DPIA เป็นต้น

DPO Outsource

ให้บริการเป็น
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือ
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

PDPA&DPO In-House Training

ให้บริการอบรมภายใน ด้วยหลักสูตรบรรยาย
และ Workshop ที่ออกแบบเฉพาะธุรกิจของคุณ
โดยผู้เชี่ยวชาญจากสถาบันพัฒนาและทดสอบ
ทักษะดิจิทัล (DDTI)

PDPA&DPO e-Learning

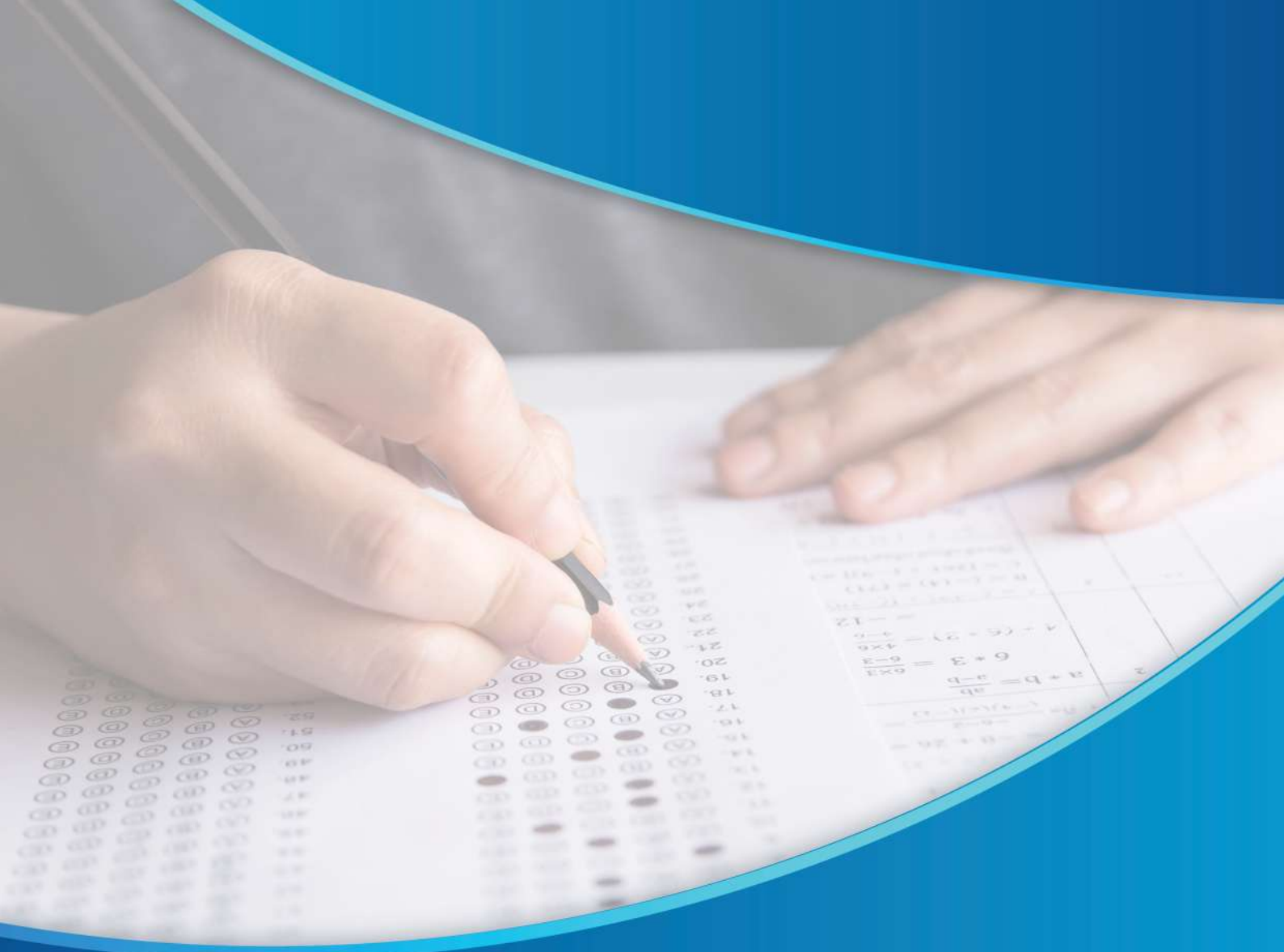
หลักสูตรออนไลน์ที่ออกแบบเนื้อหา
เกี่ยวกับ PDPA อย่างครบถ้วนและครอบคลุม
ช่วยให้พนักงานเข้าใจ PDPA อย่างง่ายดาย
สะดวก และประหยัดเวลา

บริษัท ดีบีซี กรุ๊ป จำกัด

เลขที่ 125/55 ซอยวิภาวดีรังสิต 60 แยก 12 แขวงตลาดบางเขน เขตหลักสี่ กรุงเทพฯ 10210
+66(0)2-029-0707 กด 1-5
+66(0)81-632-5918
pdpa@dbcgroup.asia
PDPA Thailand
PDPA Thailand
www.dbcgroup.asia

www.pdpathailand.com

LINE @pdpathailand



สนับสนุนโดย

ACTAP
Association of Certified Thai Accounting Practices
สมาคมสำนักงานบัญชีคุณภาพ

PDPA
THAILAND