บริษัท บีบีจีไอ จำกัด (มหาชน)

แนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล

ฉบับปรับปรุงครั้งที่ 1

วันที่ 2 กันยายน 2567

สารบัญ

1. บทนำและคำนิยาม

1.1 บทนำ

ปัจจุบัน การดำเนินงานของบริษัท บีบีจีไอ จำกัด (มหาชน) (**"บริษัทฯ"**) มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก โดยครอบคลุมเจ้าของข้อมูลส่วนบุคคลหลายกลุ่ม ได้แก่

1. ลูกค้า
2. คู่ค้า
3. พนักงาน และนักศึกษาฝึกงาน
4. ผู้สมัครงาน และผู้สมัครฝึกงาน
5. ผู้ถือหุ้น
6. ผู้มีส่วนได้เสียอื่นๆ เช่น ผู้อาศัยบริเวณใกล้เคียงโรงกลั่นน้ำมันของบริษัทฯ เยาวชนที่เข้าร่วมสโมสรฟุตบอลเยาวชนของบริษัทฯ ผู้ที่เคยเป็นพนักงานของบริษัทฯ เป็นต้น

เพื่อให้การดำเนินการใดๆ ที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทฯ จึงได้จัดทำแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่ออธิบายแนวปฏิบัติในการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย และบังคับใช้กับ ผู้บริหาร พนักงาน และลูกจ้างชั่วคราวของบริษัทฯ รวมถึงหน่วยงานภายนอกที่ให้บริการประมวลผลข้อมูลส่วนบุคคลแก่บริษัทฯ ให้ปฏิบัติตามอย่างเคร่งครัด

แนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ควรพิจารณาร่วมกับกฎบัตร นโยบาย คู่มือและประกาศที่เกี่ยวข้องดังนี้:

1. กฎบัตรการคุ้มครองข้อมูลส่วนบุคคล (DPO Charter)
2. นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Security Policy)
3. คู่มือการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Data Protection Impact Assessment หรือ DPIA)
4. คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)
5. คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)
6. คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)
7. ประกาศ เรื่อง การบันทึกข้อมูลส่วนบุคคลผ่านกล้องโทรทัศน์วงจรปิด (Closed-circuit Television (CCTV) Privacy Notice)

1.1.1 กฎหมาย ข้อบังคับ และประกาศที่เกี่ยวข้อง

แนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ จัดทำขึ้นโดยอ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งประกาศไว้ ณ วันที่ 27 พฤษภาคม พ.ศ. 2562 ทั้งนี้ หากกฎหมายฉบับดังกล่าวมีการเปลี่ยนแปลง หรือการตีความกฎหมายมีการเปลี่ยนแปลงและอาจมีผลย้อนหลัง รวมถึงกรณีที่มีการออกกฎระเบียบประกาศ คำสั่ง หลักเกณฑ์ และข้อปฏิบัติภายใต้พระราชบัญญัตินี้ บริษัทฯ จะต้องพิจารณาถึงผลกระทบของการเปลี่ยนแปลงดังกล่าวข้างต้น เพื่อทบทวนและปรับปรุงแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลนี้ ให้เหมาะสมและสอดคล้องกับกฎหมายและ/หรือการตีความกฎหมายที่เปลี่ยนแปลงไป และนำเสนอต่อคณะกรรมการบริหารและจัดการบริษัท (MANCOM) เพื่อพิจารณาอนุมัติก่อนประกาศใช้แนวปฏิบัติฉบับนี้

1.1.2 วัตถุประสงค์

การจัดทำแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มีวัตถุประสงค์หลักดังนี้

1. เพื่อให้เป็นแนวปฏิบัติในการดำเนินกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้แก่ ผู้บริหาร พนักงาน ลูกจ้างชั่วคราวของบริษัทฯ ซึ่งอยู่ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ในนามบริษัทฯ ให้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคล[1]อย่างเพียงพอและเหมาะสม เพื่อลดความเสี่ยงทั้งหลายที่อาจเกิดขึ้นต่อข้อมูลส่วนบุคคล และเพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ รวมถึงการจำกัดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
2. เพื่อเป็นแนวปฏิบัติในการจัดทำการบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity หรือ RPA) หรือ Data Inventory สำหรับบันทึกข้อมูลเกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย การเก็บรักษา และการทำลายข้อมูลส่วนบุคคล รวมถึงแนวปฏิบัติในการปรับปรุงแก้ไขข้อมูลใน Data Inventory กรณีที่มีการเปลี่ยนแปลง และเพื่อให้สามารถดำเนินการให้ข้อมูลส่วนบุคคลมีความถูกต้อง สมบูรณ์เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด
3. เพื่อเป็นแนวปฏิบัติในการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคลให้เป็นไปตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ และสามารถบริหารจัดการได้ภายในระยะเวลาตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้
4. เพื่อเป็นแนวปฏิบัติในการบริหารจัดการผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามบริษัทฯ เพื่อให้บริษัทฯ สามารถมั่นใจได้ว่าผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวมีมาตรการในการคุ้มครองดูแลข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม
5. เพื่อเป็นแนวปฏิบัติในการดำเนินการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมของบริษัทฯ ให้กลับคืนสู่สภาวะปกติโดยเร็ว และลดการเกิดผลกระทบต่อการดำเนินงานรวมถึงผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลให้น้อยที่สุด

[1] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)

1.1.3 **ขอบเขต**

แนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ให้มีผลใช้บังคับกับ ผู้บริหาร พนักงาน ลูกจ้างชั่วคราว ของบริษัทฯ รวมถึงหน่วยงานภายนอกที่ให้งานบริการแก่บริษัทฯ โดยแนวปฏิบัติฉบับนี้มีขอบเขตเนื้อหาครอบคลุม ตั้งแต่หน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง ประเภทของข้อมูลส่วนบุคคลที่อยู่ในขอบเขตการบังคับใช้ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หลักการคุ้มครองข้อมูลส่วนบุคคล ฐานทางกฎหมายสำหรับการ ประมวลผลข้อมูลส่วนบุคคล แนวปฏิบัติเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่การเก็บรวบรวม การใช้ การ เปิดเผย การเก็บรักษา และการทำลายข้อมูลส่วนบุคคล การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล การ บริหารจัดการหน่วยงานภายนอกที่ทำหน้าที่ประมวลผลให้บริษัทฯ การจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วน บุคคล รวมถึงการกำกับดูแลการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล บทลงโทษ แนวทางการทบทวนนโยบาย และแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล และแนวปฏิบัติอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

1.2 คำจำกัดความ

คำ	นิยาม
พ.ร.บ.	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศไว้ ณ วันที่ 27 พฤษภาคม พ.ศ. 2562
กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงฉบับที่ได้แก้ไขเพิ่มเติมในอนาคต และกฎ ระเบียบ ประกาศ หรือคำสั่งที่เกี่ยวข้อง
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง หรือเป็นผู้สร้างข้อมูลนั้นขึ้นมา[2]
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยเฉพาะ[3]
ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)	ข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ได้แก่ ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด[4]
การประมวลผลข้อมูลส่วนบุคคล (Processing)	การปฏิบัติการหรือส่วนหนึ่งของการปฏิบัติการซึ่งได้กระทำต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย
ข้อมูลส่วนบุคคลรั่วไหล (Personal Data Breach)	การรั่วไหลหรือละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ทำให้เกิดการประมวลผล เข้าถึง เปิดเผย ทำสำเนา เปลี่ยนแปลง เก็บ ทำซ้ำ แสดง หรือจำหน่ายข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย หรือทำให้เกิดการสูญหาย ทำลาย เปลี่ยนแปลง หรือเสียหายต่อข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูล และ/หรือ ผู้ประมวลผลข้อมูลช่วงได้ดำเนินการส่ง เก็บ หรือประมวลผลในประการอื่นอันเกี่ยวเนื่องกับการปฏิบัติตามสัญญาหลักโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย

[2] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 24

[3] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6

[4] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

คำ	นิยาม
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[5] ซึ่งมีลักษณะดังนี้ 1. เป็นผู้กำหนดวัตถุประสงค์หรือผลลัพธ์จากการประมวลผลข้อมูลส่วนบุคคล รวมถึงวิธีการประมวลผลข้อมูลส่วนบุคคล และฐานทางกฎหมายที่ใช้ 2. เป็นผู้ที่กำหนดว่าต้องประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลใด และพิจารณาผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล 3. เป็นผู้ที่ได้รับประโยชน์เชิงเศรษฐกิจหรือประโยชน์อื่นจากการประมวลผลข้อมูลส่วนบุคคล และมีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล 4. เป็นผู้กระทำการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงในสัญญาที่ได้ทำไว้กับเจ้าของข้อมูลส่วนบุคคลโดยตรง 5. เป็นผู้แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หน่วยงานภายนอกที่ทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลในนามของบริษัทฯ เช่น ทำหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บริษัทฯ[6] ซึ่งมีลักษณะดังนี้ 1. เป็นผู้ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบุคคลอื่นภายใต้ข้อตกลงในสัญญาที่ได้ทำกับผู้อื่นนั้น 2. ไม่เป็นผู้ที่กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ฐานทางกฎหมายที่ใช้ และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล 3. ไม่เป็นผู้ที่กำหนดว่าต้องประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลใด และไม่มีหน้าที่หลักในการประเมินผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล 4. เป็นผู้ที่ได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือจากผู้ควบคุมข้อมูลส่วนบุคคล และไม่เป็นผู้ที่ตัดสินใจเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล 5. ไม่เป็นผู้ที่มีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล
หน่วยงานภายนอก	ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้าง หรือผู้ให้บริการประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ และผู้ให้บริการภายนอกด้านงานทั่วไป (Service provider)
หน่วยงานภายนอกอื่น	บุคคลหรือนิติบุคคลอื่น นอกเหนือจากผู้ประมวลผลข้อมูลส่วนบุคคล
ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล	การที่เจ้าของข้อมูลส่วนบุคคลมีความสมัครใจเลือกที่จะยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของตนได้ ทั้งนี้ ความยินยอมดังกล่าวต้องมีความชัดเจน ไม่คลุมเครือ เข้าใจง่าย ไม่ล่อลวงให้เจ้าของข้อมูลส่วนบุคคลเกิดความเข้าใจผิด[7]

[5] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6

[6] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6

[7] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 59

คำ	นิยาม
ผู้เยาว์	ผู้ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 19 และ 20 แห่งประมวลกฎหมายแพ่งและพาณิชย์[8]
Record of Processing Activity (RPA) หรือ Data Inventory	การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามที่ระบุในมาตรา 39[9] หรือมาตรา 40 (3) แล้วแต่กรณี[10] เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือผู้ควบคุมข้อมูลสามารถตรวจสอบได้
การแฝงข้อมูล (Pseudonymization)	การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ ข้อมูลเพิ่มเติมนี้มีการเก็บรักษาไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรเชิงบริหารจัดการเพื่อประกันว่าข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้[11]
การจัดทำข้อมูลนิรนาม (Anonymization)	กระบวนการที่ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ ซึ่งทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลนั้นอยู่ระดับต่ำมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง[12]

[8] อ้างอิงตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 19 และ 20

[9] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 ระบุว่า ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการอย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม (7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

[10] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (3) ระบุว่า ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

[11] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 20

[12] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 20

2. หน้าที่และความรับผิดชอบ

ในการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ผู้บริหาร พนักงานและลูกจ้างของบริษัทฯ ในแต่ละหน่วยงาน จะต้องปฏิบัติตามหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ในกรณีที่บริษัทฯ มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และจะต้องปฏิบัติตามหน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ในกรณีที่บริษัทฯ มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ตามแต่ละกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ

2.1 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล

ในกรณีที่บริษัทฯ มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้บริหาร พนักงาน และลูกจ้างของบริษัทฯ ในแต่ละหน่วยงาน จะต้องปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล[13] ดังนี้

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ทั้งมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และจะต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมอยู่เสมอ โดยมาตรการดังกล่าวควรครอบคลุมถึง
    (1) มีการแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption)
    (2) มีความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล
    (3) มีความสามารถที่จะทำให้พร้อมใช้งานและการเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค
    (4) มีกระบวนการในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการอย่างสม่ำเสมอเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ
    (5) มีมาตรการควบคุมพนักงานและลูกจ้างที่ปฏิบัติงานภายใต้อำนาจของบริษัทฯ และสามารถเข้าถึงข้อมูลส่วนบุคคลได้ ไม่ให้ประมวลผลข้อมูลส่วนบุคคลโดยปราศจากคำสั่งหรือข้อกำหนดของบริษัทฯ
2. กรณีที่ต้องเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น จะต้องดำเนินการเพื่อป้องกันไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่จะทำการเก็บรักษาไว้ภายใต้ข้อยกเว้นตามกฎหมาย

[13] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 98-109

โดยออกแบบระบบในการเก็บและคัดแยกข้อมูลส่วนบุคคลที่ต้องถูกลบและทำลายภายใต้เงื่อนไขที่บริษัทฯ กำหนด และสามารถตรวจสอบได้

4. ดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment หรือ DPIA) เพื่อประเมินความเสี่ยงด้าน Data Privacy และผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรม[14]
5. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ และดำเนินการให้ข้อมูลส่วนบุคคลมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยไม่ก่อให้เกิดความเข้าใจผิด[15]
6. ดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลมีการร้องขอใช้สิทธิ ซึ่งการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลต้องไม่ชักช้า[16]และอยู่ภายในระยะเวลาที่กฎหมายกำหนด
7. ดำเนินการเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคล และมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ[17]
8. กรณีที่บริษัทฯ ใช้ผู้ประมวลผลข้อมูลส่วนบุคคลในการดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ บริษัทฯ จะต้องจัดให้มีข้อตกลงหรือสัญญาประมวลผลข้อมูล (Data Processing Agreement) เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามที่ตกลงร่วมกันระหว่างบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล และเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
9. กรณีที่บริษัทฯ จำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ บริษัทฯ จะต้องมั่นใจว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ[18]
10. ต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่
11. ให้ความร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อถูกร้องขอให้ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการชี้แจงข้อเท็จจริงตามเรื่องดังกล่าว
12. กรณีที่หน่วยงานรัฐหรือองค์กรที่ได้รับมอบหมายให้ใช้อำนาจรัฐ (“หน่วยงานของรัฐ”) มีคำร้องขอเข้าถึงข้อมูลส่วนบุคคล แต่ไม่รวมไปถึงกรณีที่บริษัทฯ มีหน้าที่ตามกฎหมายในการรายงานหรือส่งข้อมูลให้แก่ผู้กำกับดูแลตามปกติ บริษัทฯ ต้องให้หน่วยงานของรัฐดังกล่าวเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อหน่วยงานของรัฐมีอำนาจตามกฎหมายเท่านั้น หากหน่วยงานของรัฐไม่มีอำนาจตามกฎหมาย บริษัทฯ จะต้องไม่ให้หน่วยงานของรัฐเข้าถึงหรือไม่เปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานของรัฐนั้น เนื่องจากบริษัทฯ จะมีความรับผิดตามกฎหมายจากการเปิดเผยข้อมูลโดยไม่มีหน้าที่ตามกฎหมาย และบริษัทฯ ต้องจัดให้มีการยืนยันตัวตนของ

[14] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Data Protection Impact Assessment)”

[15] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 7.2 “การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory)”

[16] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)”

[17] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)”

[18] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 7.1.2.1 “การโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกในต่างประเทศ”

เจ้าหน้าที่ของหน่วยงานของรัฐก่อนอนุญาตให้เข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานของรัฐ รวมถึงจัดทำบันทึกรายการไว้ให้ครบถ้วน

13. แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล แต่หากการละเมิดนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างมาก บริษัทฯ จะต้องแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า[19]

2.2 หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล

ในกรณีที่บริษัทฯ มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ผู้บริหาร พนักงานและลูกจ้างของบริษัทฯ ในแต่ละหน่วยงาน จะต้องปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล[20] ดังนี้

1. ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงหรือสัญญาประมวลผลข้อมูล (Data Processing Agreement) หรือคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยไม่ทำการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากที่ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคล หากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร เว้นแต่คำสั่งดังกล่าวนั้นขัดต่อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
2. ไม่นำข้อมูลส่วนบุคคลภายใต้ข้อตกลงหรือสัญญาประมวลผลข้อมูลไปใช้เพื่อวัตถุประสงค์อื่น
3. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ทั้งมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว ต้องครอบคลุมเรื่อง ดังต่อไปนี้
   (1) มีการแฝงข้อมูล (Pseudonymization) หรือการเข้ารหัส (Encryption)
   (2) มีความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งานและการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล
   (3) มีความสามารถที่จะทำให้มีความพร้อมใช้งานและการเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค
   (4) มีกระบวนการทดสอบ ประเมิน และวัดผลประสิทธิภาพของมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ
   (5) มีมาตรการควบคุมพนักงานที่ประมวลผลข้อมูลส่วนบุคคลในฐานะที่บริษัทฯ เป็นผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อไม่ให้พนักงานประมวลผลข้อมูลส่วนบุคคลโดยปราศจากคำสั่งหรือข้อกำหนดของบริษัทฯ

   ทั้งนี้ ผู้บริหาร พนักงานและลูกจ้างของบริษัทฯ ในแต่ละหน่วยงาน จะต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่เห็นว่ามีทางเลือกในการประมวลผลข้อมูลส่วนบุคคลที่มีความมั่นคงปลอดภัยสูงกว่า เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงทางเลือกดังกล่าว

[19] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)”

[20] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 127-134

4. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity) ไว้ตามหลักเกณฑ์และวิธีการที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด และดำเนินการให้ข้อมูลส่วนบุคคลนั้นมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยไม่ก่อให้เกิดความเข้าใจผิด[21]
5. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบหากพบว่า การประมวลผลข้อมูลส่วนบุคคลนั้นฝ่าฝืนกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและ / หรือกฎ ระเบียบ ประกาศ หรือคำสั่งที่ออกภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
6. จัดเตรียมข้อมูลที่เหมาะสม เช่น บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและวิธีการประมวลผลข้อมูลส่วนบุคคล มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น ในลักษณะที่แสดงให้เห็นถึงการปฏิบัติตามข้อตกลงระหว่างบริษัทฯ ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล กับผู้ควบคุมข้อมูลส่วนบุคคล
7. จัดเตรียมวิธีการในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล รวมถึงความสามารถในการส่งคืน การถ่ายโอน หรือกำจัดข้อมูลส่วนบุคคล ตามวิธีการและข้อตกลงที่ระบุไว้ในสัญญากับผู้ควบคุมข้อมูลส่วนบุคคล[22]
8. ต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่
9. กรณีที่หน่วยงานรัฐหรือองค์กรที่ได้รับมอบหมายให้ใช้อำนาจรัฐ (“หน่วยงานของรัฐ”) มีคำร้องขอเข้าถึงข้อมูลส่วนบุคคล แต่ไม่รวมไปถึงกรณีที่บริษัทฯ มีหน้าที่ตามกฎหมายในการรายงานหรือส่งข้อมูลให้แก่ผู้กำกับดูแลตามปกติ บริษัทฯ จะต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบและอนุญาตก่อนให้หน่วยงานของรัฐดังกล่าวเข้าถึงข้อมูลส่วนบุคคล เนื่องจากบริษัทฯ มีความผูกพันกับผู้ควบคุมข้อมูลส่วนบุคคลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น นอกจากนี้บริษัทฯ ต้องจัดให้มีการยืนยันตัวตนของเจ้าหน้าที่ของหน่วยงานของรัฐก่อนอนุญาตให้เข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานของรัฐ รวมถึงจัดทำบันทึกรายการไว้ให้ครบถ้วน
10. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบกรณีที่มีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลเกิดการรั่วไหล โดยบริษัทฯ จะต้องทำการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าหลังจากทราบเหตุ ทั้งนี้ บริษัทฯ <u>ไม่มีหน้าที่</u>แจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำโดยอาศัยสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและบริษัทฯ

2.3 หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer หรือ DPO) มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล[23] ดังนี้

1. หน้าที่ในการให้คำแนะนำ (Duty to Inform) ได้แก่ การให้คำแนะนำและกำหนดแนวทางแก่หน่วยงานภายในบริษัทฯ รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ให้มีการแจ้งข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลทราบอย่างครบถ้วนตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงให้คำแนะนำเกี่ยวกับเนื้อหา

[21] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 7.2 “การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory)”

[22] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)”

[23] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42

หรือข้อความที่จะใช้ในการแจ้งแก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ยังมีหน้าที่ติดตามการเปลี่ยนแปลงหรือการออกใหม่ของกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงจัดให้มีการฝึกอบรม การสื่อสาร ให้ความรู้ สร้างความตระหนักรู้และนำเสนอข่าวสารเกี่ยวกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้บริษัทฯ และผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ผ่านช่องทางที่เหมาะสม

2. หน้าที่ในการให้คำปรึกษา (Duty to Advise) ได้แก่ การให้คำปรึกษาแก่หน่วยงานภายในบริษัทฯ รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ เพื่อให้การดำเนินงานของบริษัทฯ เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง รวมถึงการให้คำปรึกษาในการปรับปรุงการปฏิบัติงานเพื่อแก้ไขประเด็นข้อบกพร่องที่ตรวจพบ และการปฏิบัติตามคำแนะนำของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3. หน้าที่ในการตรวจสอบการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Duty to Ensure Compliance) ได้แก่ การวางแผนการตรวจสอบการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลประจำปีของหน่วยงานภายในบริษัทฯ และตรวจสอบการดำเนินงานของผู้บริหารและพนักงานในแต่ละหน่วยงาน รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้มีการตรวจสอบปีละ 1 ครั้ง

4. หน้าที่ในการบริหารจัดการ (Duty to Manage) ได้แก่ การจัดทำและสื่อสารแผนการดำเนินงานประจำปีแก่หน่วยงานที่เกี่ยวข้อง เพื่อให้ได้รับการสนับสนุนและการให้ความร่วมมือ การวางแผนพัฒนาศักยภาพของตนเองและ DPO Office นอกจากนี้ ยังมีหน้าที่ในการบริหารงานและกำกับดูแลการปฏิบัติงานของ DPO Office และการประสานงานกับส่วนงานต่างๆ เพื่อให้บรรลุแผนการดำเนินงานประจำปีที่กำหนด

5. หน้าที่ในการรายงาน (Duty to Report) ได้แก่ การรายงานผลการปฏิบัติงานต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่และคณะกรรมการบริหารและจัดการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือตามที่ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ หรือคณะกรรมการบริหารและจัดการบริษัทเห็นสมควร รวมถึงในกรณีที่มีเหตุการณ์ที่อาจมีผลกระทบต่อการดำเนินงานของบริษัทฯ หรือเมื่อมีการละเมิดสิทธิและเสรีภาพของบุคคลจากการรั่วไหลของข้อมูลส่วนบุคคลในระดับความเสี่ยงสูง DPO ต้องรายงานประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ทันที เพื่อให้บริษัทฯ ดำเนินการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและ/หรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อไป

6. หน้าที่ในการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Duty to Coordinate) ได้แก่ การประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยเป็นหน่วยงานกลางในการติดต่อ และในกรณีที่มีการตรวจสอบและมีคำสั่งจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้บริษัทฯ ดำเนินการใดๆ เพื่อให้สอดคล้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล DPO มีหน้าที่ในการติดตามความคืบหน้าของการดำเนินการตามคำสั่งนั้นและมีการรายงานไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในเวลาที่กำหนดไว้ในคำสั่ง นอกจากนี้ หากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในบริษัทฯ DPO มีหน้าที่แจ้งแก่สำนักงาน

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

7. หน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

ทั้งนี้ สามารถอ้างอิงรายละเอียดเพิ่มเติมเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ใน *"กฎบัตรการคุ้มครองข้อมูลส่วนบุคคล"*

3. ประเภทของข้อมูลส่วนบุคคล

ประเภทของข้อมูลส่วนบุคคลที่บังคับใช้ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สามารถจำแนกออกเป็น 2 ประเภท ดังนี้

3.1 ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคล คือ ข้อมูลใดๆ ที่เกี่ยวกับบุคคล และสามารถระบุถึงตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยความสามารถในการระบุถึงตัวบุคคลได้ แบ่งออกเป็น 3 ลักษณะ[24] คือ

1. การแยกแยะ (Distinguishability) หมายถึง การที่ข้อมูลสามารถระบุแยกแยะตัวบุคคลออกจากกันได้ เช่น ชื่อ นามสกุล หรือเลขประจำตัวประชาชน แต่หากเป็นข้อมูลอื่น เช่น คะแนนสะสมบัตรสมาชิกต่างๆ เพียงอย่างเดียวจะไม่สามารถใช้แยกแยะตัวบุคคลได้ ต้องมีข้อมูลเกี่ยวกับตัวบุคคลเพิ่มเติมเพื่อให้สามารถแยกแยะตัวบุคคลและระบุไปถึงเจ้าของข้อมูลส่วนบุคคลได้
2. การติดตาม (Traceability) หมายถึง การที่ข้อมูลสามารถถูกใช้ในการติดตามพฤติกรรมหรือกิจกรรมที่บุคคลนั้นกระทำ เพื่อระบุลักษณะจำเพาะของบุคคลนั้นได้ เช่น Log file ที่บันทึกข้อมูลกิจกรรมของผู้ใช้งานสามารถใช้ระบุถึงตัวบุคคลและติดตามพฤติกรรมของบุคคลนั้นได้
3. การเชื่อมโยง (Linkability) หมายถึง การที่ข้อมูลสามารถใช้เชื่อมโยงกันเพื่อระบุไปถึงตัวบุคคลได้ ซึ่งแบ่งออกเป็น 2 กรณี ได้แก่

   (1) ข้อมูลที่ถูกเชื่อมโยงแล้ว (Linked) คือ ข้อมูลที่ได้นำมาใช้ร่วมกันกับข้อมูลอื่นแล้ว สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ โดยข้อมูลทั้ง 2 ชุดที่จะนำมาใช้ร่วมกันนั้น มาจากแหล่งข้อมูลในระบบเดียวกันหรือระบบที่มีความเกี่ยวข้องกันอย่างใกล้ชิด และขาดการควบคุมการเข้าถึงอย่างรัดกุม โดยหากบุคคลใดที่สามารถเข้าถึงข้อมูลทั้ง 2 ชุดนั้นได้ ก็จะสามารถเชื่อมโยงข้อมูลดังกล่าวเพื่อระบุตัวเจ้าของข้อมูลส่วนบุคคลได้

   (2) ข้อมูลที่อาจถูกเชื่อมโยง (Linkable) คือ ข้อมูลที่เมื่อหากนำมาใช้ร่วมกันกับข้อมูลอื่นแล้ว มีความเป็นไปได้ว่า อาจสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมกันนั้น มาจากแหล่งข้อมูลอื่นที่ไม่อยู่ในระบบเดียวกันหรือไม่อยู่ในระบบที่มีความเกี่ยวข้องกันอย่างใกล้ชิด เช่น ได้มาจากอินเทอร์เน็ต หรือแหล่งอื่น เป็นต้น

[24] อ้างอิงตาม NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST SPECIAL PUBLICATION 800-122): GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010), at 2.1 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 24-25

ตัวอย่างของข้อมูลส่วนบุคคล[25]

1. ชื่อ นามสกุล หรือชื่อเล่น
2. ที่อยู่
3. เบอร์โทรศัพท์
4. E-mail
5. รหัสที่สามารถอ้างอิงถึงตัวเจ้าของข้อมูลส่วนบุคคล เช่น เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขประจำตัวผู้เสียภาษี เลขใบอนุญาตขับขี่ เลขบัญชีธนาคาร เลขบัตรเครดิต เป็นต้น
6. ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID
7. ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน เป็นต้น
8. ข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ เช่น วันเกิดและสถานที่เกิด สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลทางการศึกษา ข้อมูลทางการเงิน ข้อมูลจ้างงาน เป็นต้น
9. ข้อมูลการประเมินผลการทำงาน หรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
10. ข้อมูลบันทึกต่างๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆ ของบุคคล เช่น Log file
11. ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

หมายเหตุ: การเก็บภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆ ที่มีข้อมูลส่วนบุคคลนั้น ย่อมสามารถใช้ระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ จึงถือเป็นข้อมูลส่วนบุคคล

3.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม บริษัทฯ จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ โดยข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด[26] มีดังนี้

1. เชื้อชาติ หรือเผ่าพันธุ์
2. ความคิดเห็นทางการเมือง
3. ความเชื่อในศาสนา
4. พฤติกรรมทางเพศ
5. ประวัติอาชญากรรม
6. ข้อมูลสุขภาพ
7. ความพิการ
8. ข้อมูลพันธุกรรม (Genetic Data)
9. ข้อมูลชีวภาพ (Biometric Data)
10. ข้อมูลอื่นใดตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

[25] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 26

[26] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 28

4. หลักการคุ้มครองข้อมูลส่วนบุคคล

4.1 หลักการทั่วไป

4.1.1 การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมายและเป็นธรรม

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล สามารถดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะเก็บรวบรวมข้อมูลเท่านั้น โดยหากมีการเปลี่ยนแปลงหรือเพิ่มเติมวัตถุประสงค์ในภายหลัง บริษัทฯ จะต้องดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด เว้นแต่จะเป็นกรณีที่ได้รับการยกเว้นโดยกฎหมายให้สามารถทำได้โดยไม่ต้องขอความยินยอม นอกจากนี้ การประมวลผลข้อมูลส่วนบุคคลจะต้องไม่กระทบกับสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยบริษัทฯ จะต้องคุ้มครองสิทธิดังกล่าวตลอดระยะเวลาที่บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลนั้น เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมายและเป็นธรรม

4.1.2 การเก็บรักษาให้เป็นความลับและความมั่นคงปลอดภัย

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่เก็บรักษาข้อมูลส่วนบุคคลให้เป็นความลับและมีความมั่นคงปลอดภัย ไม่ว่าข้อมูลดังกล่าว จะอยู่ในรูปแบบเอกสาร หรือรูปแบบอิเล็กทรอนิกส์ก็ตาม โดยบริษัทฯ จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งครอบคลุมถึงการกำหนดแนวปฏิบัติ หรือวิธีการคณะทำงาน รวมถึงระบบปฏิบัติการที่มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเชิงเทคนิค เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหน้าที่หรือโดยมิชอบ

บริษัทฯ ต้องจัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบงานของผู้บริหาร พนักงานและลูกจ้างของบริษัทฯ อย่างเหมาะสม เพื่อให้สามารถเข้าถึงข้อมูลส่วนบุคคลได้ตามขอบเขตหน้าที่ที่รับผิดชอบเท่านั้น ซึ่งพนักงานลูกจ้างของบริษัทฯ จะต้องปฏิบัติตามหน้าที่ที่กำหนดอย่างเคร่งครัด โดยไม่นำข้อมูลส่วนบุคคลที่ตนได้เข้าถึงหรือล่วงรู้จากการปฏิบัติงานไปใช้เพื่อวัตถุประสงค์ส่วนตัวหรือทางการค้า รวมถึงไม่เปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นโดยไม่ได้รับอนุญาต หรือนำข้อมูลไปเผยแพร่ไม่ว่าจะด้วยวิธีการใด

4.1.3 การคำนึงถึงสิทธิความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบ (Privacy by Design)

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ขั้นตอนการออกแบบกระบวนการปฏิบัติงานไปจนถึงขั้นตอนการพัฒนาระบบงาน ตลอดจนการออกแบบผลิตภัณฑ์และบริการ (Privacy by Design) โดยต้องให้ความสำคัญในการสร้างความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลโดยใช้มาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการที่เหมาะสมและเพียงพอ โดยเฉพาะอย่างยิ่งในกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่อาจส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ตัวอย่างเช่น การที่บริษัทฯ กำหนดให้จัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment หรือ DPIA)[27] เพื่อวิเคราะห์ ระบุความเสี่ยง และจัดหามาตรการหรือการควบคุมเพื่อลดความ

[27] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Data Protection Impact Assessment)”

เสี่ยงก่อนจะออกผลิตภัณฑ์ หรือดำเนินการตามกระบวนการใหม่ ถือเป็นการนำหลักการ Privacy by Design มาประยุกต์ใช้

4.1.4 **ความถูกต้อง แม่นยำ และเป็นปัจจุบัน**

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการดำเนินการให้ข้อมูลส่วนบุคคลที่จัดเก็บไว้มีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด[28] โดยจัดให้มีระบบหรือขั้นตอนที่เหมาะสมในการตรวจสอบคุณภาพของข้อมูลส่วนบุคคล เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่สมบูรณ์ได้ดำเนินการลบทิ้งและได้รับการแก้ไขให้ถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ สามารถอ้างอิงรายละเอียดเกี่ยวกับแนวปฏิบัติในการปรับปรุงรายการบันทึกข้อมูลส่วนบุคคลที่จัดเก็บไว้เพิ่มเติมในหัวข้อที่ 7.2 *"การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory)"*

4.1.5 **ความโปร่งใส**[29]

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการดำเนินการประมวลผลข้อมูลส่วนบุคคลด้วยความโปร่งใส ซึ่งหมายถึงบริษัทฯ ต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลส่วนบุคคลได้รับทราบและเข้าใจถึงวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ อย่างชัดเจน โดยการแจ้งนั้น บริษัทฯ ต้องใช้ภาษาที่เข้าใจง่าย ไม่ซับซ้อน และไม่ก่อให้เกิดความเข้าใจผิด นอกจากนี้ บริษัทฯ ต้องจัดให้มีกระบวนการหรือช่องทางให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึง และตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของตนเองได้ ภายใต้ขอบเขตที่บริษัทฯ กำหนดด้วย ทั้งนี้ ในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการที่บริษัทฯ ได้มาซึ่งข้อมูลส่วนบุคคล ไม่ว่าจะได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลส่วนบุคคลหรือได้รับจากแหล่งอื่น กรณีที่บริษัทฯ ได้รับข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคล บริษัทฯ จะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลนั้น[30] แต่หากเป็นกรณีที่บริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง บริษัทฯ จะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยเร็ว และต้องไม่เกิน 30 วันนับตั้งแต่วันที่เก็บรวบรวม[31] โดยรายละเอียดที่บริษัทฯ จะต้องจัดเตรียมเพื่อแจ้งแก่เจ้าของข้อมูลส่วนบุคคลขึ้นอยู่กับแหล่งที่มาของข้อมูล ดังนี้

[28] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35

[29] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 และ 25 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guideline 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 90-93

[30] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23

[31] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25

รายละเอียดที่ต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคล	กรณีได้รับข้อมูลส่วนบุคคลจาก	
	เจ้าของข้อมูลส่วนบุคคลโดยตรง	แหล่งอื่น
ชื่อบริษัทฯ และรายละเอียดการติดต่อ	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนบริษัทฯ (ถ้ามี)	✓	✓
ข้อมูล สถานที่ติดต่อ และวิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของบริษัทฯ	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล และผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคลนั้น	✓	✓
ฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล	✓	✓
รายการของข้อมูลส่วนบุคคลที่เก็บมา	✓	✓
ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล	✓	✓
ชื่อหน่วยงานหรือบุคคลภายนอก (Third Party) ที่อาจได้รับข้อมูลส่วนบุคคลที่บริษัทฯ เปิดเผยให้	✓	✓
สิทธิของเจ้าของข้อมูลส่วนบุคคลต่อการประมวลผลข้อมูลส่วนบุคคล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	✗	✓
รายละเอียดเกี่ยวกับการที่เจ้าของข้อมูลส่วนบุคคลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่จะต้องให้ข้อมูลแก่บริษัท (ถ้ามี)	✓	✗

4.2 หลักการเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น

บริษัทฯ กำหนดแนวทางในการปฏิบัติเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยให้ยึดหลักการเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น[32] ดังนี้

1. เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (Necessity)
2. เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการประมวลผลข้อมูล (Relevance)
3. เก็บรวบรวมข้อมูลส่วนบุคคลในปริมาณที่จำกัดเท่าที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล และเก็บรักษาข้อมูลส่วนบุคคลตามระยะเวลาที่จำเป็นเพื่อการประมวลผลข้อมูลส่วนบุคคล หรือตามที่กฎหมายกำหนดเท่านั้น (Limitation)

อย่างไรก็ตาม การพิจารณาความจำเป็น ต้องคำนึงถึงกรณีที่เกี่ยวข้องกับการเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามข้อกำหนด ข้อบังคับ และเพื่อการตรวจสอบ เช่น บริษัทฯ อาจมีความจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลไว้เกินระยะเวลาที่จำเป็นเพื่อการประมวลผลข้อมูลส่วนบุคคล สำหรับกรณีที่จำเป็นต้องใช้ดำเนินการตามคำสั่งศาล หรือหน่วยงานที่กำกับดูแล เป็นต้น

แต่ละหน่วยงานของบริษัทฯ ควรพิจารณาดำเนินการตามแนวปฏิบัติดังต่อไปนี้ เพื่อให้แน่ใจว่ามีการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล และเก็บรักษาตามระยะเวลาที่จำเป็นหรือตามที่กฎหมายกำหนด[33] ดังนี้

1. กำหนดคำสั่ง หรือฟังก์ชั่นของระบบที่ใช้ในการประมวลผลข้อมูล ให้บันทึกและจัดเก็บเฉพาะข้อมูลที่จำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
2. สอบทานอย่างสม่ำเสมอว่าข้อมูลส่วนบุคคลที่ใช้ในการประมวลผลมีความเพียงพอ เกี่ยวข้องและจำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลหรือไม่ หากไม่จำเป็นต้องลบหรือทำลายข้อมูล และไม่เก็บรวบรวมอีกต่อไป
3. พิจารณาว่ากิจกรรมหรือกระบวนการทำงานนั้น สามารถหลีกเลี่ยงการนำข้อมูลส่วนบุคคลมาใช้ในการประมวลผลได้หรือไม่ รวมถึงพิจารณาใช้ข้อมูลรวม (Aggregated Data) เช่น ข้อมูลทางสถิติ ซึ่งไม่ถือเป็นข้อมูลส่วนบุคคล ในการประมวลผลตามวัตถุประสงค์ของกิจกรรมแทน เป็นต้น
4. สอบทานและปรับปรุงแบบฟอร์มให้มีช่องสำหรับกรอกข้อมูลที่จำเป็นเท่านั้น
5. ปิดทับข้อมูลที่ไม่จำเป็นให้ไม่สามารถมองเห็นหรืออ่านได้
6. ใช้การแฝงข้อมูลส่วนบุคคล (Pseudonymization)[34] ก่อนจัดเก็บข้อมูลส่วนบุคคลในฐานข้อมูล เพื่อให้ไม่สามารถระบุถึงตัวตนของเจ้าของข้อมูลส่วนบุคคลได้
7. จัดทำข้อมูลนิรนามหรือลบข้อมูลส่วนบุคคลทันทีที่ไม่มีความจำเป็นต้องใช้ (Anonymization and Deletion)
8. กำหนดให้ระบบที่จัดเก็บข้อมูลส่วนบุคคล หรือฐานข้อมูลส่วนบุคคล มีการแจ้งเตือนเมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

[32] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 ระบุว่า การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

[33] อ้างอิงตาม Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, The European Data Protection Board (EDPB)

[34] การแฝงข้อมูลส่วนบุคคล หมายถึง การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ ข้อมูลเพิ่มเติมนี้มีการเก็บรักษาไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรเชิงบริหารจัดการเพื่อประกันว่าข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้

ทั้งนี้ บริษัทฯ สามารถอ้างอิงแนวทางในการเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลในหัวข้อที่ 7.1.3 *"การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล"* และ สามารถอ้างอิงแนวทางการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้เมื่อพ้นระยะเวลาการเก็บรักษาในหัวข้อที่ 7.1.4 *"การทำลายข้อมูลส่วนบุคคล"*

5. ฐานในการประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลจะสามารถดำเนินการได้โดยชอบด้วยกฎหมายเมื่อมี "ฐานทางกฎหมาย" (Lawful basis) รองรับการดำเนินกิจกรรมการประมวลผลข้อมูลดังกล่าว ไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเปิดเผย การเก็บรักษา และการทำลายข้อมูลส่วนบุคคล โดยในการประมวลผลข้อมูลส่วนบุคคลแต่ละครั้ง บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะต้องระบุฐานทางกฎหมายที่ใช้เพื่อการประมวลผลข้อมูลส่วนบุคคล[35] พร้อมทั้งแจ้งฐานในการประมวลผลให้เจ้าของข้อมูลส่วนบุคคลทราบ แล้วจึงดำเนินการกับข้อมูลนั้นตามฐานการประมวลผลซึ่งมีข้อจำกัดที่แตกต่างกัน ทั้งนี้ บริษัทฯ ต้องจัดให้มีบันทึกการใช้ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลแต่ละชุดอย่างเป็นลายลักษณ์อักษร

นอกเหนือจากการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Consent) ซึ่งเป็นฐานหนึ่งในการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้ว บริษัทฯ สามารถใช้ฐานทางกฎหมายอื่นเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคล ซึ่งมีทั้งหมด 6 ฐาน ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล[36] ได้แก่

1. ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research)
2. ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
3. ฐานการปฏิบัติตามสัญญา หรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา (Contract)
4. ฐานภารกิจของรัฐ (PublicTask)
5. ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) และ
6. ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

ในการประมวลผลข้อมูลส่วนบุคคลของแต่ละกิจกรรม อาจใช้ฐานทางกฎหมายเพื่อรองรับการประมวลผลข้อมูลดังกล่าวได้มากกว่าหนึ่งฐาน โดยการประมวลผลข้อมูลส่วนบุคคลตามฐานทางกฎหมายที่แตกต่างกันนั้น จะส่งผลให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิแตกต่างกันไปตามข้อจำกัดหรือเงื่อนไขของแต่ละฐาน

[35] ตามข้อมูลเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ณ วันที่ 27 พ.ค. 63 มีฐานทางกฎหมายที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ได้แก่ ฐานความยินยอม ฐานการปฏิบัติตามสัญญา ฐานประโยชน์โดยชอบด้วยกฎหมาย และฐานการปฏิบัติตามกฎหมาย

[36] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 และคำอธิบายเพิ่มเติมอ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 53

5.1 ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research)

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะใช้ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติเพื่อประมวลผลข้อมูลส่วนบุคคลได้ เมื่อการประมวลผลข้อมูลนั้นจำเป็นต่อการบรรลุวัตถุประสงค์ของการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลจากการอ้างอิงฐานนี้ จะต้องอ้างอิงฐานทางกฎหมายอื่นร่วมด้วย[37]

หากบริษัทฯ จะใช้ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติเพื่อประมวลผลข้อมูลส่วนบุคคล บริษัทฯ จะต้องจัดให้มีมาตรการปกป้องข้อมูลส่วนบุคคลที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยต้องเป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งควรสอดคล้องกับมาตรฐานจริยธรรมของระเบียบวิธีในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัยและสถิติของการศึกษาประเภทต่างๆ ด้วย เพื่อให้การส่งต่อข้อมูลหรือนำไปใช้งานต่อในบริบทอื่นๆ สามารถทำได้โดยง่าย และถูกต้องตามเงื่อนไขของกฎหมายของประเทศอื่นๆ เช่นกัน โดยมาตรฐานจริยธรรมดังกล่าว ได้ถือปฏิบัติตามแนวทางสากล ทั้งยังมีความสอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ หลักความจำเป็น หลักความได้สัดส่วน และการเคารพสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล[38]

5.2 ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะใช้ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล เพื่อประมวลผลข้อมูลส่วนบุคคลได้ เมื่อการประมวลผลข้อมูลส่วนบุคคลนั้นมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคล เช่น เพื่อป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) บริษัทฯ จะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลส่วนบุคคลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตของเจ้าของข้อมูลส่วนบุคคลได้นอกจากการประมวลผลข้อมูลส่วนบุคคลโดยบริษัทฯ

5.3 ฐานการปฏิบัติตามสัญญา หรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา (Contract)

การใช้ฐานการปฏิบัติตามสัญญาหรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญาเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจำเป็นต่อการปฏิบัติตามสัญญาที่ตกลงกันไว้ระหว่างบริษัทฯ และเจ้าของข้อมูลส่วนบุคคลหรือไม่ หรือการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้นหรือไม่ โดยหากเป็นการประมวลผลข้อมูลส่วนบุคคลบนฐานการปฏิบัติตามสัญญาหรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา จะต้องกำหนดให้

[37] สามารถอ่านรายละเอียดเพิ่มเติมจาก Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 84

[38] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 85

ครอบคลุมเฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญากับทางบริษัทฯ เท่านั้น ไม่ให้หมายความรวมถึงการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่สาม ซึ่งอาจมีการอ้างอิงถึงในเนื้อหาของสัญญา เนื่องจากการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่สามดังกล่าว จะกระทำได้โดยการใช้ฐานความยินยอม (Consent) หรือฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) แล้วแต่กรณี แต่ไม่สามารถใช้ฐานการปฏิบัติตามสัญญาหรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา (Contract) เพื่อการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่สามได้ ทั้งนี้ ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องประเมินว่าผลประโยชน์ที่เกิดแก่คู่สัญญาหรือบริษัทฯ นั้นไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลที่เป็นบุคคลที่สาม และไม่เกินขอบเขตที่เจ้าของข้อมูลส่วนบุคคลที่เป็นบุคคลที่สามสามารถคาดหมายได้อย่างสมเหตุสมผล[39]

นอกจากนี้ ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ต้องประเมินและระบุขอบเขตของสัญญาให้เจ้าของข้อมูลส่วนบุคคลทราบอย่างแน่ชัดว่า ขอบเขตของรายการข้อมูลส่วนบุคคลที่บริษัทฯ จำเป็นต้องใช้ในการปฏิบัติตามสัญญา และขอบเขตการประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามสัญญามีเพียงใด

ทั้งนี้ ในกรณีที่บริษัทฯ ใช้ผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อดำเนินการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตของสัญญา จะถือว่าการประมวลผลข้อมูลส่วนบุคคลดังกล่าวใช้ฐานการปฏิบัติตามสัญญาหรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา ดังนั้น ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพิ่มเติมอีก

5.4 **ฐานภารกิจของรัฐ** (Public Task)

การใช้ฐานภารกิจของรัฐเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย ซึ่งเจ้าหน้าที่หรือองค์กรของรัฐมักใช้ฐานนี้ในการประมวลผลข้อมูลส่วนบุคคล เช่น สำนักงานศาลยุติธรรม สำนักงานเลขาธิการสภาผู้แทนราษฎรและวุฒิสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่โดยใช้อำนาจที่รัฐได้มอบหมายให้เพื่อผลประโยชน์สาธารณะตามกฎหมาย เช่น การให้บริการสอบใบอนุญาตขับขี่รถยนต์ เป็นต้น โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจน และสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

ในกรณีที่บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลตามฐานภารกิจของรัฐนี้ เจ้าของข้อมูลส่วนบุคคลจะไม่มีสิทธิในการขอให้บริษัทฯ ดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุถึงเจ้าของข้อมูลได้ รวมถึงไม่มีสิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น อย่างไรก็ตาม เจ้าของข้อมูลส่วนบุคคลยังคงมีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้

[39] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 54

5.5 ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

การใช้ฐานประโยชน์โดยชอบด้วยกฎหมายเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องพิจารณาถึง**ความจำเป็น**ที่บริษัทฯ ต้องได้รับผลลัพธ์ซึ่งเป็นประโยชน์โดยชอบด้วยกฎหมายจากการประมวลผลข้อมูลส่วนบุคคลนั้น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้อย่างสมเหตุสมผล และไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ดังนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ต้องใช้ดุลยพินิจอย่างรอบคอบในการ**ประเมินความสมดุล**ระหว่าง (1) ประโยชน์โดยชอบด้วยกฎหมายที่บริษัทฯ จะได้รับและความจำเป็นของการประมวลผลข้อมูลส่วนบุคคล กับ (2) ผลกระทบที่อาจเกิดขึ้นต่อสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล เพื่อให้การประมวลผลข้อมูลส่วนบุคคล เป็นไปอย่างเพียงพอเหมาะสม และได้สัดส่วนกับผลกระทบต่อสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ดังกล่าวนั้น

ดังนั้น หากผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาแล้วว่าจะใช้ฐานประโยชน์โดยชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมใดกิจกรรมหนึ่ง ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องประเมินและพิจารณาว่า

1. มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลในการประมวลผลข้อมูลตามวัตถุประสงค์จริง
2. ผลประโยชน์โดยชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคลดังกล่าวนั้นมีความชัดเจน
3. ต้องชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบด้วยกฎหมายของบริษัทฯ กับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล โดยการจัดทำการประเมินความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessments หรือ LIA) ซึ่งพิจารณาถึงปัจจัยเหล่านี้[40] อย่างครบถ้วน
    (1) ลักษณะของข้อมูลส่วนบุคคลและผลประโยชน์ ซึ่งอาจขึ้นอยู่กับความสัมพันธ์ระหว่างบริษัทฯ กับเจ้าของข้อมูลส่วนบุคคล เพื่อให้เข้าใจว่าเจ้าของข้อมูลส่วนบุคคลมีความคาดหวังอย่างไรต่อการจัดการข้อมูลส่วนบุคคลนั้น
    (2) ผลกระทบและความเสี่ยงที่จะเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล เช่น การเปิดเผยข้อมูลต่อบุคคลอื่น เป็นต้น
    (3) มาตรการปกป้องข้อมูลส่วนบุคคลและคุ้มครองสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างของกิจกรรมที่บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลโดยใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย เช่น การบันทึกภาพด้วยระบบกล้องวงจรปิด โดยมีวัตถุประสงค์เพื่อบันทึกภาพการทำงานของพนักงาน และเพื่อสิทธิประโยชน์ของพนักงานในการรักษาความปลอดภัย และใช้เป็นหลักฐานในกรณีที่เกิดเหตุการณ์ผิดปกติ โดยการดำเนินการดังกล่าว มีความสมดุลระหว่าง ประโยชน์โดยชอบด้วยกฎหมายที่บริษัทฯ จะได้รับ และมิได้กระทบกระเทือนถึงสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเกินควร[41]

[40] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 80

[41] อ้างอิงรายละเอียดเกี่ยวกับการประมวลผลโดยการใช้กล้องวงจรปิดเพิ่มเติมตาม “Closed-circuit Television (CCTV) Privacy Notice”

5.6 **ฐานการปฏิบัติตามกฎหมาย** (Legal Obligation)

การใช้ฐานการปฏิบัติตามกฎหมายเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจำเป็นต่อการปฏิบัติหน้าที่ตามที่กฎหมายกำหนดหรือไม่ โดยผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องสามารถระบุได้อย่างชัดเจนว่าการประมวลผลข้อมูลส่วนบุคคลดังกล่าว เป็นการปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมายหรือตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจทางกฎหมาย

ในกรณีที่บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลโดยใช้ฐานการปฏิบัติตามกฎหมาย เจ้าของข้อมูลส่วนบุคคลจะไม่มีสิทธิในการขอให้บริษัทฯ ดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุถึงเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงไม่มีสิทธิในการขอโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น หรือขอคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้[42]

[42] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 76

6. ความยินยอมเพื่อการประมวลผลข้อมูลส่วนบุคคล (Consent)

6.1 การขอความยินยอมเพื่อประมวลผลข้อมูลส่วนบุคคล

ในกรณีที่บริษัทฯ ไม่สามารถใช้ฐานทางกฎหมายอื่นใด ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ประมวลผลข้อมูลส่วนบุคคลได้[43] บริษัทฯ ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆ โดยในการขอความยินยอมบริษัทฯ ต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม นอกจากนี้ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) บริษัทฯ จะทำได้ก็ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่จะเข้าข้อกำหนดใน พ.ร.บ.[44] โดยรายละเอียดจะแสดงในหัวข้อที่ 6.2 การขอความยินยอมโดยชัดแจ้ง (Explicit Consent)

6.1.1 ข้อกำหนดในการขอความยินยอม

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล บริษัทฯ ต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ดังนั้น เมื่อต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้บริหารและพนักงานของแต่ละหน่วยงานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้ เพื่อให้แน่ใจว่าการขอความยินยอมเป็นไปตามที่ พ.ร.บ. กำหนด[45]

1. บริษัทฯ ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ก่อนการประมวลผลข้อมูลส่วนบุคคล
2. การขอความยินยอมสามารถทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้
3. ข้อความในการขอความยินยอมต้องมีความชัดเจน ไม่คลุมเครือ เข้าใจง่าย ไม่ล่อลวงให้เกิดความเข้าใจผิด (Clear Affirmative Action) เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกให้ความยินยอมโดยสมัครใจ และต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้ล่วงหน้า เช่น Pre-ticked box ซึ่งไม่ถือเป็นความยินยอมที่ชัดเจน เป็นต้น
4. หากเป็นการขอความยินยอมจากผู้เยาว์ต้องใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่าย และต้องได้รับความยินยอมจากผู้ปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย เว้นแต่ เป็นไปตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 และมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์[46] ผู้เยาว์จึงจะสามารถให้ความยินยอมตามลำพังได้[47] ทั้งนี้ บริษัทฯ อาจใช้วิธีการแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม หรือกำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental setting หรือ parental mode) เพื่อป้องกันไม่ให้ผู้เยาว์ให้ข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์

---

[43] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 5 "ฐานในการประมวลผลข้อมูลส่วนบุคคล"

[44] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ระบุว่า ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรมข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อกำหนดตาม มาตรา 26 (1) - (5)

[45] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 58-65

[46] อ้างอิงตามมาตรา 22 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อหลุดพ้นจากหน้าที่อันใดอันหนึ่ง
มาตรา 23 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการต้องทำเองเฉพาะตัว
มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการสมแก่ฐานานุรูปแห่งตน และเป็นการอันจำเป็นในการดำรงชีพอันสมควร

[47] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 20 (1)

5. ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการหรือเป็นผลของความจำเป็นในการปฏิบัติตามสัญญา และต้องแยกส่วนกับเงื่อนไขในการให้บริการอย่างชัดเจน[48]
6. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่ขอความยินยอม ต้องมีความเฉพาะเจาะจง โดย
   (1) ไม่สามารถเพิ่มเติมวัตถุประสงค์ใหม่ โดยไม่ขอความยินยอมใหม่ได้
   (2) การประมวลผลข้อมูลส่วนบุคคลหลายประเภทเพื่อวัตถุประสงค์เดียวกัน สามารถขอความยินยอมครั้งเดียวได้
   (3) กรณีที่จำเป็นต้องใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ จะต้องให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกได้ว่าให้ความยินยอมหรือปฏิเสธการให้ความยินยอมสำหรับแต่ละวัตถุประสงค์
7. ต้องเปิดเผยชื่อหน่วยงานหรือบุคคลภายนอก (Third Party) ซึ่งมีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมต่อการประมวลผลข้อมูลส่วนบุคคลนั้น
8. ออกแบบทางเลือกให้เจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะให้ความยินยอมได้ รวมถึงสามารถถอนความยินยอมได้โดยง่ายเช่นเดียวกับการให้ความยินยอม และต้องมีวิธีแจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบถึงผลกระทบจากการถอนความยินยอมดังกล่าว
9. ชี้แจงประโยชน์ที่จะเกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลให้ความยินยอม เช่น จะทำให้ประสบการณ์การใช้บริการสะดวกรวดเร็วมากขึ้น เป็นต้น และควรอธิบายเกี่ยวกับมาตรการรักษามั่นคงความปลอดภัยข้อมูลส่วนบุคคลของบริษัทฯ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมีความไว้วางใจและยินยอมให้ประมวลข้อมูลส่วนบุคคลได้[49]

[48] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 4

[49] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 58

6.2 การขอความยินยอมโดยชัดแจ้ง (Explicit Consent)

ในการประมวลผล**ข้อมูลส่วนบุคคลที่มีความอ่อนไหว** (Sensitive Personal Data) ซึ่งไม่เข้าข้อยกเว้นตามที่ระบุใน พ.ร.บ. มาตรา 26 (1) - (5)[50] บริษัทฯ ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้นอกจากการปฏิบัติตามข้อกำหนดในการขอความยินยอมที่ระบุในข้อ 6.1.1 แล้ว หน่วยงานต้องระบุรายการข้อมูลส่วนบุคคลและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล**อย่างชัดเจนและเป็นลายลักษณ์อักษร** โดยรูปแบบการขอความยินยอมโดยชัดแจ้ง มีดังนี้[51]

1. การขอความยินยอมโดยชัดแจ้งในรูปแบบเอกสาร ต้องกำหนดให้เจ้าของข้อมูลส่วนบุคคลลงลายมือชื่อกำกับเพื่อเป็นหลักฐานยืนยันการให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว
2. การขอความยินยอมโดยชัดแจ้งด้วยช่องทางอิเล็กทรอนิกส์ ต้องกำหนดให้มีวิธีการยืนยันการให้ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เช่น กำหนดให้เจ้าของข้อมูลส่วนบุคคลแนบไฟล์เอกสารที่มีการลงลายมือชื่อ หรือให้ลงลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

6.3 การบริหารจัดการความยินยอม

6.3.1 การจัดการความยินยอมที่ได้รับ

1. การบันทึกรายละเอียดเกี่ยวกับการได้มาซึ่งความยินยอม

   เมื่อบริษัทฯ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว **บริษัทฯ ต้องบันทึกรายละเอียดเกี่ยวกับการได้มาซึ่งความยินยอม**[52]จากเจ้าของข้อมูลส่วนบุคคลแต่ละรายเพื่อเป็นหลักฐานการให้ความยินยอม และสามารถบริหารจัดการกับความยินยอมได้อย่างเป็นระบบ **การบันทึกรายละเอียดเกี่ยวกับการได้มาซึ่งความยินยอมต้องครอบคลุมหัวข้อดังนี้**

   (1) ข้อมูลที่ระบุถึงตัวตนของผู้ให้ความยินยอม เช่น ชื่อ-นามสกุล Online Username เป็นต้น

   (2) วันที่ที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

[50] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ระบุว่า ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

[51] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 63

[52] หน่วยงานต้องบันทึกรายละเอียดการจัดเก็บความยินยอมในระบบ Consent Management tool ของบริษัทฯ เพื่อความถูกต้อง แม่นยำในการนำข้อมูลส่วนบุคคลไปประมวลผลตามที่ได้แจ้งขอความยินยอมไว้

(3) วิธีการที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม เช่น การให้ความยินยอมโดยการลงนามบนกระดาษ ผ่านช่องทางอิเล็กทรอนิกส์ การให้ความยินยอมทางวาจาหรือจากบทสนทนาโดยการบันทึกเสียง เป็นต้น

(4) รายละเอียดของความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ ณ ขณะนั้น

2. การติดตามและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่ได้รับความยินยอม

2.1. ความยินยอมที่ได้รับหลังจาก พ.ร.บ. มีผลบังคับใช้

บริษัทฯ กำหนดให้ผู้บริหารและพนักงานดำเนินการติดตามและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างสม่ำเสมอ โดยใช้ระบบบริหารจัดการคำยินยอม (Consent management tool) เป็นเครื่องมือในการติดตามและตรวจสอบ เพื่อให้แน่ใจว่าการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้เท่านั้น[53]

2.2. ความยินยอมที่เก็บรวบรวมไว้ก่อน พ.ร.บ. มีผลบังคับใช้

บริษัทฯ ต้องกำชับให้หน่วยงานที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนวันที่ พ.ร.บ. มีผลบังคับใช้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม[54] หากเจ้าของข้อมูลส่วนบุคคลไม่ได้แจ้งยกเลิก หรือเปลี่ยนแปลงความยินยอมในวัตถุประสงค์เดิมดังกล่าว ทั้งนี้ บริษัทฯ กำหนดให้ผู้บริหารและพนักงานดำเนินการติดตามและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างสม่ำเสมอ โดยใช้ระบบบริหารจัดการคำยินยอม (Consent management tool) เป็นเครื่องมือในการติดตามและตรวจสอบ เพื่อให้แน่ใจว่าการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้เท่านั้น

นอกจากการดำเนินการที่ระบุในหัวข้อ 2.1 และ 2.2 แล้ว บริษัทฯ ต้องทบทวนความความเหมาะสมของระยะเวลาที่ความยินยอมมีผลบังคับใช้โดยพิจารณาจากวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล รายละเอียดของความยินยอม และความคาดหวังของเจ้าของข้อมูลส่วนบุคคล[55] เช่น ระยะเวลาของความยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของสมาชิก ไม่ควรเกินไปกว่าระยะเวลาอายุการเป็นสมาชิก เนื่องจากความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ตอนสมัครสมาชิกนั้น เจ้าของข้อมูลส่วนบุคคลประสงค์จะให้บริษัทฯ ใช้ข้อมูลเท่าที่ยังมีสถานะเป็นสมาชิก เว้นแต่มีข้อยกเว้นให้ต้องเก็บข้อมูลส่วนบุคคลไว้ เช่น ตามหน้าที่ในกฎหมายอื่น เป็นต้น ทั้งนี้ หากพิจารณาแล้วพบว่าระยะเวลาที่ความยินยอมมีผลบังคับใช้นั้นสิ้นสุดลง บริษัทฯ ต้องหยุดการประมวลผลข้อมูลส่วนบุคคลดังกล่าว

[53] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21 ระบุว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่
(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว
(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

[54] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 95 ระบุว่า ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้อ งกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

[55] อ้างอิงตาม Guide to the General Data Protection Regulation (GDPR), Consent, The Information Commissioner's Office in the UK (ICO)

6.3.2 การถอนความยินยอม

การถอนความยินยอมเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลสามารถปฏิบัติได้ตลอดระยะเวลาที่บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลอันเป็นผลมาจากการได้รับความยินยอมนั้น โดยบริษัทฯ กำหนดช่องทางการเปลี่ยนแปลงสิทธิที่เกี่ยวกับความยินยอม เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำร้องขอใช้สิทธิ ดังแสดงในตารางด้านล่าง

เจ้าของข้อมูลส่วนบุคคล	ช่องทางการเปลี่ยนแปลงสิทธิที่เกี่ยวกับความยินยอม
ลูกค้า / คู่ค้า / อื่น ๆ	Call Center เบอร์ 0-2335-8899
	BBGI-secretary@bbgigroup.com
พนักงานปัจจุบัน	BBGI-HR@bbgigroup.com
	BBGI-secretary@bbgigroup.com
อดีตพนักงาน	BBGI-HR@bbgigroup.com
	BBGI-secretary@bbgigroup.com
ผู้ถือหุ้น / นักลงทุน	IR@bbgigroup.com
	BBGI-secretary@bbgigroup.com

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิในการถอนความยินยอม ผู้บริหารและพนักงานของหน่วยงานที่มีหน้าที่รับผิดชอบต่อการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่เกี่ยวกับความยินยอมดังกล่าว ต้องดำเนินการดังต่อไปนี้[56]

1) แจ้งผลกระทบของการถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ กรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด[57]
2) ระงับการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับวัตถุประสงค์ของความยินยอมดังกล่าวโดยทันที[58]
3) ลบข้อมูลส่วนบุคคลดังกล่าว หากบริษัทฯ ไม่มีความจำเป็นหรือไม่มีฐานกฎหมายอื่นๆ ที่จะรองรับการประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป[59]

นอกจากนี้ กรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิที่อาจส่งผลกระทบต่อความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ก่อนหน้า[60] ได้แก่ สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล และสิทธิในการลบข้อมูลส่วนบุคคล ผู้บริหารและพนักงานของหน่วยงานที่มีหน้าที่รับผิดชอบต่อการประมวลผลข้อมูลส่วนบุคคลนั้น ต้องดำเนินการดังต่อไปนี้[61]

[56] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 8 "การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล" และ สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมใน "คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)"

[57] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 6

[58] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34

[59] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 (2)

[60] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรค 6

[61] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 8 "การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล" และ สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมใน "คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)"

1) กรณีใช้สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล ต้องระงับการใช้ข้อมูลส่วนบุคคลในฐานข้อมูลที่เกี่ยวข้อง เว้นแต่มีเหตุให้สามารถดำเนินการใช้ข้อมูลดังกล่าวได้ต่อไป โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่น การใช้ข้อมูลเพื่อการปฏิบัติตามสัญญาระหว่างบริษัทฯ และเจ้าของข้อมูลส่วนบุคคล หรือเพื่อป้องกันอันตรายต่อชีวิตของเจ้าของข้อมูลส่วนบุคคล เป็นต้น[62]
2) กรณีใช้สิทธิในการลบข้อมูลส่วนบุคคล ให้ดำเนินการลบข้อมูลส่วนบุคคลดังกล่าว หากบริษัทฯ ไม่มีอำนาจตามกฎหมายที่จะประมวลผลข้อมูลนั้นได้ต่อไป[63]

ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ การถอนความยินยอมอาจต้องได้รับความยินยอมจากผู้ปกครองผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจปกครองตามกฎหมาย เว้นแต่ กรณีที่การถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจถอนความยินยอมได้เอง[64]

[62] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34

[63] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 (2)

[64] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 20 วรรค 4

7. การบริหารจัดการข้อมูลส่วนบุคคล

7.1 วงจรข้อมูลส่วนบุคคล (Personal Data Life Cycle)

7.1.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ต้องแจ้งขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ยอมรับหรืออนุญาตก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดๆ[65] ในกรณีที่บริษัทฯ ไม่สามารถใช้ฐานทางกฎหมายอื่นเพื่อรองรับการประมวลผลข้อมูลส่วนบุคคลดังกล่าว[66]

ทั้งนี้ ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องดำเนินการเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และไม่เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า[67]

ในกรณีที่มีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ จะต้องขอความยินยอมโดยชัดแจ้ง (Explicit consent)[68] จากเจ้าของข้อมูลส่วนบุคคลนั้น ก่อนดำเนินการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว เว้นแต่กรณีต่อไปนี้[69]

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
2. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
3. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
4. เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    (1) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของบริษัทฯ หรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์
    (2) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่อ อันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักรหรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และ

[65] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 6 “การขอความยินยอมเพื่อการประมวลผลข้อมูลส่วนบุคคล”

[66] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 5 “ฐานในการประมวลผลข้อมูลส่วนบุคคล”

[67] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 4.3 “การแจ้งและเปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล”

[68] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 6.2 “การขอความยินยอมโดยชัดแจ้ง (Explicit Consent)”

[69] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

เสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(3) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐาน และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) การศึกษาวิจัยทางวิทยาศาสตร์ สถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

(5) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

7.1.2 การใช้และการเปิดเผยข้อมูลส่วนบุคคล

สำหรับการใช้และการเปิดเผยข้อมูลส่วนบุคคล ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะต้องดำเนินการดังต่อไปนี้

1. ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะเก็บรวบรวม รวมถึงได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (ในกรณีที่บริษัทฯ อาศัยฐานความยินยอมในการใช้และเปิดเผยข้อมูลส่วนบุคคล)[70]
2. จำกัดการใช้ข้อมูลส่วนบุคคล ให้มีการใช้งานเฉพาะส่วนที่เกี่ยวข้องและจำเป็นสำหรับวัตถุประสงค์ที่กำหนด ทั้งในด้านการจำกัดรายละเอียดของข้อมูลส่วนบุคคลเพื่อให้ตรงกับวัตถุประสงค์การใช้งาน (Data Minimization) และการจำกัดผู้บริหารและพนักงานที่สามารถเข้าถึงและ/หรือใช้ข้อมูลส่วนบุคคล (Limited Access) ให้มีเฉพาะผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล สามารถเข้าถึงและ/หรือใช้ข้อมูลส่วนบุคคลได้ เท่านั้น
3. จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลหรือตามที่กฎหมายกำหนด (Data Minimization) หรือจัดทำข้อมูลนิรนามเพื่อให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Anonymization) และบันทึกผลการดำเนินการดังกล่าว
4. ควบคุมให้การส่งข้อมูลส่วนบุคคลบนเครือข่ายที่มีมาตรการความมั่นคงปลอดภัยที่เหมาะสม โดยผู้บริหารและพนักงานของบริษัทฯ ต้องดำเนินการเพื่อให้มั่นใจได้ว่ามีเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบการส่งข้อมูลส่วนบุคคลได้ เพื่อให้ข้อมูลส่วนบุคคลนั้นไม่ถูกบิดเบือนและถูกส่งไปยังผู้รับที่ถูกต้อง
5. บันทึกการถ่ายโอนหรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นหรือหน่วยงานภายนอกอื่น เพื่อเป็นหลักฐานแสดงถึงการทำงานร่วมกันกับบุคคลอื่นหรือหน่วยงานภายนอกอื่นดังกล่าว และเพื่อเป็นการ

[70] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 และ 21

สนับสนุนคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลในอนาคต ผู้บริหารและพนักงานของบริษัทฯ ต้องระบุรายละเอียดภายในบันทึกดังกล่าว ดังต่อไปนี้

(1) ข้อมูลส่วนบุคคลใดบ้างที่ถูกถ่ายโอนหรือเปิดเผย

(2) การเปิดเผยข้อมูลส่วนบุคคลนั้นได้ถ่ายโอนหรือเปิดเผยไปยังใครและเมื่อใด

(3) แหล่งที่มาของการเปิดเผยและการอนุญาตให้ทำการเปิดเผยข้อมูลส่วนบุคคล ในกรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลเพิ่มเติมจากการทำงานปกติ เช่น การเปิดเผยที่มาจากการสอบสวนที่ถูกต้องตามกฎหมายหรือการตรวจประเมินจากภายนอก เป็นต้น

(4) หน่วยงานภายในและชื่อบุคคลที่เป็นผู้เปิดเผยข้อมูลส่วนบุคคล

6. พิจารณาถึงเหตุจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นหรือหน่วยงานภายนอกอื่น[71] ไม่ว่าจะด้วยวิธีการส่งข้อมูลส่วนบุคคลหรืออนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลในระบบสารสนเทศของบริษัทฯ
7. ดำเนินการตรวจสอบและกำกับดูแล เพื่อให้มั่นใจว่าบุคคลอื่นหรือหน่วยงานภายนอกอื่นที่รับโอนหรือเปิดเผยข้อมูลส่วนบุคคลไปให้ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งในเชิงบริหารจัดการและเชิงเทคนิคอย่างเพียงพอ

7.1.2.1 การโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกอื่นในต่างประเทศ

ในกรณีที่บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีความจำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกอื่นในต่างประเทศ ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ต้องพิจารณาว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หรือมีนโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หากพนักงานมีข้อสงสัยเกี่ยวกับการดำเนินการดังกล่าว ควรขอคำปรึกษาจาก DPO / DPO Office ด้านการคุ้มครองข้อมูลส่วนบุคคล ก่อนดำเนินการโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกอื่นในต่างประเทศนั้นๆ

อย่างไรก็ตาม การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอนั้นสามารถทำได้หากเป็นข้อยกเว้นตามพ.ร.บ.[72] ดังนี้

1. กรณีจำเป็นต้องปฏิบัติตามหน้าที่ทางกฎหมาย
2. กรณีได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลให้ทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางที่รับข้อมูลส่วนบุคคลแล้ว
3. กรณีจำเป็นต้องปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
4. กรณีเป็นการปฏิบัติตามสัญญาระหว่างบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นในต่างประเทศ เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

[71] ยกเว้นกรณีที่เป็นการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลตามหน้าที่ทางกฎหมาย อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21 (2)

[72] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28

5. กรณีเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6. กรณีจำเป็นต้องดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ทั้งนี้ ผู้บริหารและพนักงานของบริษัทฯ ต้องระบุและจัดทำเอกสารการปฏิบัติตามข้อกำหนด กฎหมาย และ/หรือ ระเบียบข้อบังคับที่ขึ้นกับเขตอำนาจทางกฎหมาย หรือองค์กรระหว่างประเทศที่ข้อมูลจะถูกถ่ายโอน เพื่อใช้เป็นหลักฐานสำหรับการถ่ายโอนข้อมูลส่วนบุคคลระหว่างเขตอำนาจกฎหมาย

นอกจากนี้ ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ ต้องระบุและจัดทำเอกสารเกี่ยวกับประเทศและองค์กรระหว่างประเทศที่ข้อมูลส่วนบุคคลสามารถถูกถ่ายโอนได้ เพื่อส่งมอบให้แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่ถูกร้องขอ

สำหรับกรณีการโอนข้อมูลส่วนบุคคลไปยังบริษัทในเครือกิจการหรือเครือธุรกิจเดียวกันที่ต่างประเทศ หากประเทศปลายทางยังไม่มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล ผู้บริหารและพนักงานในแต่ละหน่วยงานของบริษัทฯ อาจพิจารณาใช้นโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules) เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันได้ โดยนโยบายดังกล่าวต้องได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว[73]

อย่างไรก็ตาม หากเกิดกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทาง ให้บริษัทฯ เสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ[74]

7.1.3 การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ ต้องเก็บข้อมูลส่วนบุคคลไว้นาน**เท่าที่จำเป็น หรือเพื่อปฏิบัติตามฐานทางกฎหมายเท่านั้น** โดยจะต้องพิจารณาเหตุผลอันสมควรในการเก็บรักษาข้อมูลส่วนบุคคลซึ่งควรสอดคล้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล หรือฐานทางกฎหมายที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เช่น เพื่อทำตามสัญญา เพื่อให้บริการตามข้อตกลง หรือเพื่อประโยชน์โดยชอบด้วยกฎหมาย เป็นต้น นอกจากนี้ ระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลขึ้นอยู่กับความเหมาะสมของแต่ละหน่วยงานของบริษัทฯ ซึ่งอาจพิจารณาให้สอดคล้องตามระเบียบข้อบังคับ แนวปฏิบัติ คำสั่งที่ออกภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการแก้ไขเพิ่มเติมกฎหมายใดๆ หรือการออกกฎหมายใดๆ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นครั้งคราว

ทั้งนี้ หากบริษัทฯ ไม่มีฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล บริษัทฯ จะต้องดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ โดยวิธีการอาจแตกต่างกันไป ขึ้นอยู่กับประเภทของข้อมูลส่วนบุคคล

[73] เนื่องจากบริษัทฯ ยังไม่มีกิจกรรมการโอนข้อมูลส่วนบุคคลตามกรณีดังกล่าว จึงยังไม่มีการปฏิบัติจริงตามแนวปฏิบัติที่ระบุไว้นี้ อย่างไรก็ตาม หากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการเปลี่ยนแปลง หรือการตีความกฎหมายมีการเปลี่ยนแปลงและอาจมีผลย้อนหลัง รวมถึงกรณีที่มีการออกกฎระเบียบ ประกาศ คำสั่ง หลักเกณฑ์ และข้อปฏิบัติภายใต้พระราชบัญญัตินี้ บริษัทฯ จะต้องพิจารณาทบทวนและปรับปรุงแนวปฏิบัติฉบับนี้ ให้เหมาะสมและสอดคล้องกับกฎหมายและ / หรือการตีความกฎหมายที่เปลี่ยนแปลงไป

[74] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28

ลักษณะการจัดเก็บ และลักษณะการใช้งาน ซึ่งสามารถอ้างอิงรายละเอียดเพิ่มเติมในหัวข้อที่ 7.1.4 *"การทำลายข้อมูลส่วนบุคคล"*

7.1.3.1 การจัดเก็บข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล ในรูปแบบดังนี้

รูปแบบ	สถานที่จัดเก็บของบริษัทฯ
เอกสารที่เป็นกระดาษ	• ตู้เอกสาร • ห้องเก็บสัญญา • คลังเก็บเอกสาร
ข้อมูลอิเล็กทรอนิกส์	• เครื่องคอมพิวเตอร์ • เครื่องแม่ข่าย (Server) • Shared drive ของส่วนงาน / ฝ่ายงาน • Cloud • สื่อบันทึกข้อมูล (media) เช่น USB, Memory card, CD, External Hard disk

ในการจัดเก็บข้อมูลส่วนบุคคล ผู้บริหารและพนักงานของบริษัทฯ ต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่บริษัทฯ กำหนด เช่น ต้องเก็บเอกสารไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงของบุคคลอื่น โดยการใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย[75] สำหรับข้อมูลอิเล็กทรอนิกส์ต้องกำหนดให้มีการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศที่จัดเก็บข้อมูลส่วนบุคคล การควบคุมการเข้ารหัสข้อมูล การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม[76] โดยเฉพาะข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ต้องมีการจัดเก็บและดูแลรักษาตามมาตรการที่กำหนดอย่างเข้มงวดมากขึ้น เช่น เอกสารข้อมูลผลตรวจสุขภาพและเอกสารประวัติอาชญากรรมของผู้รับเหมาต้องจัดเก็บในตู้เอกสารที่มีกุญแจล็อคตลอดเวลา และกำหนดให้เฉพาะผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคลดังกล่าวเป็นผู้ถือกุญแจเท่านั้น หากเป็นข้อมูลอิเล็กทรอนิกส์ต้องมีการเข้ารหัส (Encrypted) และจัดเก็บในโฟลเดอร์ที่มีการกำหนดสิทธิในการเข้าถึง และทบทวนสิทธิในการเข้าถึงอย่างสม่ำเสมอ เป็นต้น

7.1.3.2 ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้แต่ละหน่วยงานต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลที่เหมาะสม โดยคำนึงถึงความจำเป็นตามวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลนั้นๆ เว้นแต่กรณีดังต่อไปนี้

1. เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น[77]
2. เก็บรักษาไว้เพื่อวัตถุประสงค์ตามข้อกำหนด ดังต่อไปนี้

[75] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน "คู่มือวิธีปฏิบัติในการบริหารจัดการและควบคุมข้อมูลภายในบริษัทฯ"

[76] อ้างอิงตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และ มาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารเทศ

[77] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรค 2

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล[78]

(2) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัทฯ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่บริษัทฯ[79]

(3) เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ[80]

1) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของบริษัทฯ หรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

2) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

3. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย[81]

ทั้งนี้ การกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลของแต่ละหน่วยงาน อาจพิจารณาจากกรอบระยะเวลาในการเก็บรักษา ตามตารางด้านล่างนี้ เพื่อเป็นแนวทางในการกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลอย่างเหมาะสม

เอกสารหรือไฟล์ที่มีข้อมูลส่วนบุคคล	ข้อพิจารณาเกี่ยวกับกรอบระยะเวลาการเก็บรักษา
สัญญา เช่น สัญญาซื้อขาย สัญญาการให้บริการ สัญญาเช่า เป็นต้น	อายุสัญญา เงื่อนไขและข้อตกลงที่เกี่ยวข้อง และกฎหมายที่เกี่ยวข้องกับธุรกรรมดังกล่าว อายุความตามกฎหมาย
เอกสารที่ออกโดยหน่วยงานราชการ หรือเอกสารที่ต้องยื่นต่อหน่วยงานราชการ	ตามข้อกำหนดของหน่วยงานราชการที่เกี่ยวข้อง อายุความตามกฎหมาย
เอกสารที่เกี่ยวข้องกับคดีความ	อายุความตามกฎหมาย
สัญญาจ้างพนักงาน และเอกสารหรือไฟล์ที่มีข้อมูลส่วนบุคคลของพนักงาน	ตลอดระยะเวลาตามสัญญาจ้าง และกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 กำหนดให้เก็บรักษาทะเบียนพนักงานไม่น้อยกว่า 2 ปี นับแต่วันสิ้นสุดของการจ้างของพนักงานแต่ละราย และสำหรับเอกสารเกี่ยวกับ การจ่ายค่าจ้าง ค่าล่วงเวลา ค่าทำงานในวันหยุด และค่าล่วงเวลาใน

[78] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (1)

[79] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (4) และ 32 (3)

[80] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 (5) (ก) และ (ข)

[81] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32 (1) (ข)

เอกสารหรือไฟล์ที่มีข้อมูลส่วนบุคคล	ข้อพิจารณาเกี่ยวกับกรอบระยะเวลาการเก็บรักษา
	วันหยุดให้เก็บรักษาไว้ไม่น้อยกว่า 2 ปี นับแต่วันจ่ายเงิน อายุความตามกฎหมาย
บันทึกจากกล้องวงจรปิด CCTV หรือรูปภาพ หรือวิดีโอ	วัตถุประสงค์ของกิจกรรม และ/หรือฐานทางกฎหมายที่เกี่ยวข้อง อายุความตามกฎหมาย
เอกสารเกี่ยวกับการเงินและการบัญชี เช่น ใบแจ้งหนี้ ใบเสร็จรับเงิน เป็นต้น	ไม่น้อยกว่า 5 ปีนับแต่วันปิดบัญชีหรือจนกว่าจะมีการส่งมอบบัญชี ตามที่กำหนดโดยพระราชบัญญัติการบัญชี พ.ศ. 2543 อายุความตามกฎหมาย
เอกสารทางภาษี เช่น ใบกำกับภาษีและสำเนาใบกำกับภาษี เป็นต้น	ไม่น้อยกว่า 5 ปีนับแต่วันที่ได้ยื่นแบบแสดงรายการภาษีหรือวันทำรายงานแล้วแต่กรณี ตามมาตรา 87/3 แห่งประมวลรัษฎากร อายุความตามกฎหมาย

นอกจากนี้ บริษัทฯ กำหนดให้แต่ละหน่วยงานต้องทำการทบทวนระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลง เพื่อให้แน่ใจว่าระยะเวลาการเก็บรักษาที่กำหนดนั้นยังมีความเหมาะสม สอดคล้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลและข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

7.1.4 การทำลายข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้ผู้บริหารและพนักงานดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ เมื่อเข้ากรณีดังต่อไปนี้

1. เมื่อข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2. เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามที่บริษัทฯ และแต่ละหน่วยงานกำหนดไว้และไม่มีกฎหมายใดระบุให้จัดเก็บต่อไป
3. เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ หรือได้ถอนความยินยอม โดยบริษัทฯ ไม่มีฐานทางกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป[82]
4. เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยบริษัทฯ ไม่อาจปฏิเสธได้ตามเกณฑ์ที่ พ.ร.บ. กำหนด[83]
5. เมื่อพบว่าข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

ในกรณีที่บริษัทฯ ได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องดำเนินการดังกล่าว ทั้งในทางปฏิบัติ และทางเทคโนโลยีด้วยค่าใช้จ่ายของบริษัทฯ เอง ทั้งยังมี

[82] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)”

[83] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)”

หน้าที่ต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นๆ ตามสัญญาแบ่งปันข้อมูล (Data Sharing Agreement) (ถ้ามี) เพื่อให้ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลนั้น[84]

อย่างไรก็ตาม บริษัทฯ อาจมีความจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์บางประการตามที่ได้ระบุในหัวข้อ 7.1.3.2 ข้อ 1. – 3. ทั้งนี้ หากหน่วยงานมีข้อสงสัยเกี่ยวกับแนวปฏิบัติในการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ ผู้บริหารและพนักงานของหน่วยงานดังกล่าวควรพิจารณาขอคำปรึกษาจากฝ่ายกฎหมาย (LC) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามความเหมาะสมแล้วแต่กรณี

ตัวอย่างวิธีการทำลายข้อมูลส่วนบุคคล ตามรูปแบบการจัดเก็บข้อมูล มีดังนี้

รูปแบบการจัดเก็บข้อมูลส่วนบุคคล	ตัวอย่างวิธีการทำลาย
กระดาษ หรือแฟ้มเอกสาร	ย่อยโดยเครื่องย่อยเอกสาร หรือใช้บริการหน่วยงานภายนอก
ข้อมูลอิเล็กทรอนิกส์ เช่น ในอีเมล์ shared drive หรือคอมพิวเตอร์ของพนักงาน หรือคอมพิวเตอร์ส่วนตัว หรือฐานข้อมูล หรือ Cloud	ลบ หรือ การจัดทำข้อมูลนิรนาม หรือ การแฝงข้อมูลส่วนบุคคล
สื่อบันทึกข้อมูล เช่น CD DVD เป็นต้น	ทุบทำลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut
สื่อบันทึกข้อมูล เช่น USB, Memory card, และ External hard disk	ทุบทำลาย หรือ Dumping ข้อมูล หรือใช้ซอฟต์แวร์ลบข้อมูลที่เทียบเท่ามาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา

1. การแฝงข้อมูลส่วนบุคคล (Pseudonymization) คือ วิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่างๆ เป็นต้น ด้วยชื่อหรือรหัสที่สร้างขึ้นมาด้วยวิธีการใดวิธีการหนึ่งอันเป็นเอกลักษณ์ และได้เก็บรักษาข้อมูลทั้งสองชุดไว้แยกจากกัน ซึ่งทำให้การประมวลผลข้อมูลส่วนบุคคลแฝง ไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ การแฝงข้อมูลส่วนบุคคลจึงเป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลตั้งต้น[85]

2. การจัดทำข้อมูลนิรนาม (Anonymization) คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง เนื่องจากเป็นข้อมูลส่วนบุคคลที่ผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้ โดยวิธีการจัดทำข้อมูลนิรนาม สามารถแบ่งออกเป็น 4 วิธี[86] คือ
   (1) การจัดทำข้อมูลนิรนามแบบเป็นทางการ (Formal Anonymization) คือการกำจัด หรือซ่อนตัวระบุเจ้าของข้อมูลส่วนบุคคลโดยตรงออกจากตัวข้อมูล
   (2) การจัดทำข้อมูลนิรนามแบบได้รับการรับรอง (Guaranteed Anonymization) คือ การจัดทำข้อมูลนิรนามโดยชุดของสมมติฐานใดสมมติฐานหนึ่ง ซึ่งเป็นสมมติฐานบนความรู้เบื้องต้นของผู้ล่วงละเมิด

[84] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรค 3

[85] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 28 และ 260

[86] อ้างอิงตาม Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562 หน้า 256-259

(3) การจัดทำข้อมูลนิรนามทางสถิติ (Statistical Anonymization) คือ การจัดทำข้อมูลนิรนามที่ลดความน่าจะเป็นในการระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลย้อนหลังให้ต่ำลง ซึ่งไม่ถึงกับทำให้ความน่าจะเป็นดังกล่าวเป็นศูนย์ แต่ลดความเสี่ยงของข้อมูลให้ถึงระดับที่เหมาะสม เช่น วิธีการผสมข้อมูล (Scrambling) วิธีการปิดทับข้อมูล (Masking) วิธีการลดความชัดเจนของข้อมูลลง (Blurring or Noising) เป็นต้น

(4) การจัดทำข้อมูลนิรนามในเชิงการใช้งาน (Functional Anonymization) คือ การจัดทำข้อมูลนิรนามในเชิงสถิติโดยพิจารณาร่วมกับปัจจัยอื่นๆ ที่อาจส่งผลต่อความเสี่ยงของการระบุตัวเจ้าของข้อมูลส่วนบุคคล เช่น แรงจูงใจของผู้รุกล้ำข้อมูลส่วนบุคคล (Intruder's motivation) ผลกระทบของการถูกเปิดเผยของข้อมูลนิรนาม (Consequence of re-identification) โอกาสที่จะเกิดเหตุการณ์ที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยไม่ตั้งใจ (Spontaneous identification) ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลส่วนบุคคลกับผู้มีหน้าที่จัดการข้อมูลส่วนบุคคล เป็นต้น

บริษัทฯ กำหนดให้แต่ละหน่วยงานจัดให้มีระบบหรือวิธีการการตรวจสอบการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นระยะเวลาที่บริษัทฯ กำหนด เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลถูกลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ตามวิธีและภายในระยะเวลาที่กำหนดอย่างมีประสิทธิผล กล่าวคือข้อมูลส่วนบุคคลที่ลบหรือทำลายไม่สามารถกู้คืนหรือนำมาทำให้สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้อีก

สำหรับกรณีที่บริษัทฯ ว่าจ้างหน่วยงานภายนอกทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาที่บริษัทฯ กำหนด บริษัทฯ ต้องกำหนดให้หน่วยงานภายนอกดังกล่าว จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมในการทำลายข้อมูลส่วนบุคคลตามที่บริษัทฯ กำหนดและระบุข้อตกลงที่จำเป็นในสัญญาจ้างอย่างเหมาะสม ตามแต่ละกรณี[87] รวมถึงต้องมีการขอหนังสือรับรองหรือหลักฐานการทำลายข้อมูลส่วนบุคคล เช่น รูปภาพ เป็นต้น

[87] กรณีที่มีการว่าจ้างหน่วยงานหรือบุคคลภายนอกทำลายข้อมูลส่วนบุคคล หน่วยงานควรปรึกษาฝ่ายกฎหมาย (LC) / สายงานกำกับองค์กร (CC) สำหรับกรณีที่เกี่ยวข้องกับสัญญาและข้อตกลงเพิ่มเติม

7.2 การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory)

บริษัทฯ กำหนดให้แต่ละหน่วยงานจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity (RPA) หรือ Data Inventory)[88] เพื่อใช้บันทึกข้อมูลเกี่ยวกับกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของแต่ละหน่วยงาน ตั้งแต่การเก็บรวบรวม ใช้ เปิดเผย ตลอดจนการเก็บรักษาและการทำลายข้อมูลส่วนบุคคล เพื่อให้สามารถทราบถึงวงจรของข้อมูลส่วนบุคคล (Personal Data Cycle) ของแต่ละกิจกรรมได้อย่างเป็นระบบ และเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยพนักงานในแต่ละหน่วยงานที่เป็นเจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล มีหน้าที่จัดทำบันทึกรายละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลลงใน Data Inventory ให้มีความถูกต้องสมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด ทั้งนี้ ผู้บริหารของแต่ละหน่วยงานมีหน้าที่รับผิดชอบในการกำกับดูแลและสอบทานความถูกต้องและความครบถ้วนของข้อมูลดังกล่าว

พนักงานในแต่ละหน่วยงานต้องบันทึกรายการข้อมูลดังหัวข้อต่อไปนี้ ลงในบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory)

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6. การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
7. การปฏิเสธคำขอหรือการคัดค้านการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล[89]
8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย
9. สถานที่จัดเก็บข้อมูล ทั้งรูปแบบที่เป็นเอกสารและรูปแบบอิเล็กทรอนิกส์
10. ประเภทของเจ้าของข้อมูลส่วนบุคคล เช่น ลูกค้า พนักงาน คู่ค้า เป็นต้น
11. หน่วยงานภายในบริษัทฯ ที่สามารถเข้าถึงข้อมูลส่วนบุคคลของแต่ละกิจกรรม
12. ฐานทางกฎหมายที่ใช้ประมวลผลข้อมูลส่วนบุคคลของแต่ละกิจกรรม

เพื่อให้การบันทึกข้อมูลใน Data Inventory มีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด บริษัทฯ กำหนดให้พนักงานในแต่ละหน่วยงานที่เป็นเจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ดำเนินการทบทวน Data Inventory อย่างน้อยปีละ 1 ครั้ง หรือเมื่อการประมวลผลข้อมูลส่วนบุคคลมีการเปลี่ยนแปลง โดยดำเนินการตามขั้นตอนดังต่อไปนี้

[88] ทะเบียนบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) ถูกจัดเก็บเป็นแบบ centralized โดยมีการจำกัดสิทธิให้ Process Owner มีสิทธิในการเข้าถึงและเปลี่ยนแปลงข้อมูลได้เฉพาะข้อมูลที่หน่วยงานของตนเองรับผิดชอบ สำหรับ DPO จะมีสิทธิในการเข้าถึงได้ตลอดเวลาของทุกหน่วยงาน

[89] การปฏิเสธคำขอหรือการคัดค้านฯ จะบันทึกในทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล โดยสามารถเชื่อมโยงมายังรายชื่อกิจกรรมที่เกี่ยวข้องใน Data Inventory ทั้งนี้ สามารถอ้างอิงรายละเอียดใน "คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)"

1. เมื่อถึงกำหนดรอบการทบทวน Data Inventory พนักงานในแต่ละหน่วยงานที่เป็นเจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อมูลใน Data Inventory ของตน ที่จัดเก็บอยู่ในระบบ Centralized ให้ครอบคลุมตามหัวข้อที่ระบุไว้ข้างต้น โดยหากพบว่ามีข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วน พนักงานจะต้องดำเนินการแก้ไขข้อมูลส่วนบุคคลที่บันทึกไว้ให้ถูกต้องและตรงกับการปฏิบัติงานจริง รวมถึงต้องเพิ่มเติมการบันทึกข้อมูลส่วนบุคคลดังกล่าวให้ครบถ้วนสมบูรณ์ ตามลำดับ
2. ในกรณีที่กิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการเปลี่ยนแปลง พนักงานในแต่ละหน่วยงานที่เป็นเจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล จะต้องปรึกษากับผู้บริหารของหน่วยงานของตน DPO และ DPO Office โดยประสานงานร่วมกับ PDPA Champion เพื่อให้ได้ข้อสรุปว่าสามารถดำเนินการเปลี่ยนแปลงกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ แล้วจึงปรับปรุงข้อมูลใน Data Inventory ของตนในระบบ Centralized ให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนแปลงไป
3. เมื่อพนักงานในแต่ละหน่วยงานได้ดำเนินการทบทวน Data Inventory ให้มีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดแล้ว จะต้องแจ้ง PDPA Champion เพื่อประสานงานให้ผู้บริหารของหน่วยงานสอบทาน Data Inventory ในระบบ Centralized
4. กรณีที่ผู้บริหารของหน่วยงานมีความเห็นให้ปรับปรุง Data Inventory เพิ่มเติม PDPA Champion จะต้องเป็นตัวแทนในการประสานงานไปยังพนักงานที่เกี่ยวข้องให้ดำเนินการปรับปรุงแก้ไข
5. เมื่อ Data Inventory ได้รับการสอบทานความถูกต้องและความครบถ้วนจากผู้บริหารของหน่วยงานแล้ว PDPA Champion จะต้องแจ้งการทบทวนและปรับปรุง Data Inventory ในระบบ Centralized แก่ DPO และ DPO Office เพื่อดำเนินการตรวจสอบต่อไป

7.3 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

เนื่องด้วยบริษัทฯ ตระหนักถึงความสำคัญของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล บริษัทฯ จึงกำหนดให้ผู้บริหารและพนักงานในแต่ละหน่วยงานมีหน้าที่รับผิดชอบในการจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม ทั้งทางด้านที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (IT) และทางด้านที่ไม่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (Non-IT) โดยผู้บริหารและพนักงานต้องปฏิบัติตามระเบียบ ข้อบังคับที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามที่บริษัทฯ กำหนดอย่างเคร่งครัด เช่น นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ มาตรการรักษาความลับ รวมถึงนโยบายและแนวปฏิบัติอื่นๆ ที่เกี่ยวข้อง เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลสูญหาย ถูกเข้าถึง นำไปใช้ เปลี่ยนแปลง แก้ไข ทำลาย หรือนำไปเปิดเผยโดยมิชอบหรือปราศจากความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

นอกจากนี้ บริษัทฯ กำหนดให้ผู้บริหารและพนักงานในแต่ละหน่วยงานจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เข้มงวดมากขึ้น สำหรับการประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

1. ข้อมูลส่วนบุคคลที่มีความอ่อนไหว[90] เช่น ข้อมูลสุขภาพ เป็นต้น
2. ข้อมูลส่วนบุคคลอื่นที่อาจก่อให้เกิดความเสียหายหรือเกิดผลกระทบต่อสิทธิและเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างมาก เช่น หมายเลขบัตรเครดิตหรือเดบิต เป็นต้น
3. ข้อมูลส่วนบุคคลของผู้เปราะบาง[91] เช่น ผู้เยาว์ ผู้สูงอายุ บุคคลกลุ่มเฉพาะที่ต้องการความคุ้มครองเป็นพิเศษ เช่น ผู้ป่วยทางจิต ผู้อพยพลี้ภัย ผู้สูงอายุ หรือผู้ป่วย เป็นต้น

ทั้งนี้ บริษัทฯ พิจารณากำหนดให้แต่ละหน่วยงานกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยอาจแบ่งตามประเภทหรือระดับชั้นความสำคัญของข้อมูล (Data classification) ซึ่งได้แก่ Secret Data Confidential Data, Internal Use only Data และ Public Data ตามความเหมาะสมในแต่ละหน่วยงาน เพื่อเป็นแนวทางในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลได้อย่างเพียงพอและเหมาะสม

เนื่องด้วยข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของบริษัทฯ จะอยู่ภายใต้การคุ้มครองความเป็นส่วนตัว (Privacy) และภายใต้การรักษาข้อมูลให้เป็นความลับ (Confidentiality) ตามมาตรการรักษาความลับของบริษัทฯ ผู้บริหารและพนักงานจึงต้องปฏิบัติตามข้อกำหนด ดังนี้

1. ห้ามมิให้ผู้บริหารและพนักงานประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ เปิดเผย และ/หรือทำลายข้อมูลส่วนบุคคลโดยที่ไม่ได้รับอนุญาต หรือโดยมิชอบ[92] หรือโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. ห้ามมิให้ผู้บริหารและพนักงานนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์ส่วนตัวหรือทางการค้า
3. ห้ามมิให้นำข้อมูลส่วนบุคคลไปเผยแพร่ไม่ว่าจะด้วยวิธีการใดก็ตาม
4. กำหนดสิทธิและจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลตามความเหมาะสม แล้วแต่กรณี[93]

---

[90] สามารถอ้างอิงรายละเอียดเพิ่มเติมในหัวข้อที่ 3.2 “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว”

[91] อ้างอิงจากสำนักจริยธรรมการวิจัย คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่, จริยธรรมการวิจัยสำหรับนักวิจัย (Version 1.0 December, 2015): “บุคคลเปราะบาง” (vulnerable persons)” หมายถึง (1) บุคคลที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากขาดอำนาจการศึกษาทรัพยากร, ความเข้มแข็ง หรืออื่น ๆ (2) บุคคลที่ถูกชักจูงเข้าร่วมการวิจัยโดยง่าย โดยหวังจะได้ประโยชน์จากการเข้าร่วม ไม่ว่าจะสมเหตุสมผลหรือไม่ก็ตาม หรือเป็นผู้ตกลงเข้าร่วมการวิจัยเพราะเกรงกลัวจะถูกกลั่นแกล้งจากผู้มีอำนาจเหนือกว่าหากปฏิเสธ

[92] ผู้บริหารและพนักงานจะประมวลผลข้อมูลส่วนบุคคลได้ เฉพาะภายใต้ขอบเขตที่ได้รับอนุญาตหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

[93] ตามตารางสิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Access control matrix) ที่แต่ละหน่วยงานกำหนด โดยอาศัยหลักการ “จำเป็นต้องรู้” (Need-to-Know) กล่าวคือ ผู้บริหารและพนักงานจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้ เฉพาะส่วนที่มีความจำเป็นต่อการประมวลผลข้อมูล ภายใต้ขอบเขตงานที่กำหนด

บริษัทฯ กำหนดให้แต่ละหน่วยงานต้องทำการทบทวนมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งทางด้านที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (IT) และทางด้านที่ไม่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (Non-IT) อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรการดังกล่าวยังมีความเพียงพอและเหมาะสม สอดคล้องกับระเบียบ ข้อบังคับที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่บริษัทฯ กำหนด

นอกจากนี้ บริษัทฯ ได้กำหนดให้ผู้บริหารในแต่ละหน่วยงานมีหน้าที่รับผิดชอบต่อการกำกับดูแลการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และกำหนดให้ผู้บริหารและพนักงานทุกหน่วยงานมีหน้าที่รับผิดชอบต่อการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลที่อาจเกิดจากมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไม่เพียงพอและเหมาะสม โดยผู้บริหารและพนักงานต้องปฏิบัติตามกลไกหรือกระบวนการที่ใช้สำหรับการบริหารจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล ตามแนวปฏิบัติที่บริษัทฯ กำหนด[94]

ทั้งนี้ หากพบการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามที่ระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ หรือพบเหตุละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคล ผู้บริหารและพนักงานต้องดำเนินการแจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทันที หรือโดยไม่ชักช้านับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้[95]

[94] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)”

[95] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 10 “การจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล”

8. การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้ผู้บริหารและพนักงานของหน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ต้องจัดเตรียมข้อมูลและสถานที่ รวมถึงกลไกหรือกระบวนการเพื่อใช้สำหรับรองรับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และกำหนดให้ผู้บริหารและพนักงานปฏิบัติตามคำร้องขอฯ ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด ซึ่งกลไกหรือกระบวนการเพื่อใช้สำหรับรองรับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลต้องครอบคลุมคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ดังนี้

1. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
2. สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
3. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล
4. สิทธิในการลบข้อมูลส่วนบุคคล
5. สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล
6. สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล
7. สิทธิในการถอนความยินยอม[96]

บริษัทฯ กำหนดให้แต่ละหน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล บันทึกคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล[97] และกำหนดให้มีการติดตามสถานะคำร้องและการดำเนินการตามคำร้อง ดังกล่าวในทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล

เมื่อบริษัทฯ ได้รับคำร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล บริษัทฯ กำหนดให้แต่ละหน่วยงานที่มีหน้าที่รับผิดชอบต่อการตอบสนองต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้าภายหลังการยืนยันตัวตนของผู้ยื่นคำร้องใช้สิทธิและการพิจารณาแล้วว่าเข้าเงื่อนไขในการดำเนินการของบริษัทฯ โดยผู้บริหารและพนักงานของหน่วยงานต้องดำเนินการตามขั้นตอนที่บริษัทฯ กำหนด[98] ให้แล้วเสร็จภายใน 20 วันนับแต่วันที่ได้รับคำร้องขอ[99]

ผู้บริหารและพนักงานของบริษัทฯ ต้องปฏิบัติตามขั้นตอนในการตอบสนองคำร้องขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยสามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมจาก *"คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)"* ซึ่งระบุขั้นตอนในการดำเนินการไว้ดังนี้

1. การรับคำร้องของเจ้าของข้อมูลส่วนบุคคล
2. การยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล

---

[96] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเพิ่มเติมในหัวข้อที่ 6.3.2 "การถอนความยินยอม"

[97] ทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคลถูกจัดเก็บเป็นแบบ centralized โดยมีการจำกัดสิทธิให้หน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและเปลี่ยนแปลงข้อมูลได้เฉพาะข้อมูลที่หน่วยงานของตนเองรับผิดชอบ สำหรับ DPO จะมีสิทธิในการเข้าถึงและเปลี่ยนแปลงข้อมูลที่รับผิดชอบโดยหน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตลอดเวลาของทุกหน่วยงาน

[98] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน "คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)" หัวข้อที่ 6.2.5 การดำเนินการตามคำร้อง

[99] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. มาตรา 30 ระบุว่าให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำร้องขอตามสิทธิในการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ สำหรับระยะเวลาในการดำเนินการตามคำร้องขอตามสิทธิประเภทอื่นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้ระบุไว้ อย่างไรก็ตามเพื่อให้การดำเนินการตามคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคลไม่ล่าช้ากว่าที่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด บริษัทฯ จึงกำหนดให้การดำเนินการดังกล่าวให้แล้วเสร็จภายใน 20 วันนับแต่วันที่ได้รับคำขอของเจ้าของข้อมูลส่วนบุคคล

3. การพิจารณาคำร้อง
4. การแจ้งยืนยันเพื่อดำเนินการตามคำร้อง
5. การดำเนินการตามคำร้อง
6. การปิดสถานะคำร้องเมื่อเสร็จสิ้นการดำเนินการ
7. การติดตามสถานะคำร้องและการดำเนินการตามคำร้อง

บริษัทฯ สามารถกำหนดให้ผู้บริหารและพนักงานของหน่วยงานปฏิเสธคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ด้วยเหตุผลตามที่ระบุไว้ใน พ.ร.บ. โดยมีเงื่อนไขการปฏิเสธคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล สรุปได้ดังนี้

ข้อที่	สิทธิของเจ้าของข้อมูลส่วนบุคคล	เงื่อนไขในการปฏิเสธคำร้อง
1	สิทธิในการเข้าถึงข้อมูลส่วนบุคคล	1. เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้น ส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิเสรีภาพของบุคคลอื่น
2	สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล	1. การประมวลผลนั้นเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือการดำเนินการตามคำร้องดังกล่าวละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น
3	สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล	1. เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย 2. บริษัทฯ ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล สามารถพิสูจน์ได้ว่าการประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์สาธาณะ หรือเพื่อประโยชน์โดยชอบด้วยกฎหมาย ที่ไม่ได้ขอความยินยอมนั้นจากเจ้าของข้อมูลส่วนบุคคล มีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล 3. เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัทฯ
4	สิทธิในการลบข้อมูลส่วนบุคคล	1. การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น 2. การประมวลผลเป็นไปเพื่อให้บรรลุวัตถุประสงค์ในการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ข้อที่	สิทธิของเจ้าของข้อมูลส่วนบุคคล	เงื่อนไขในการปฏิเสธคำร้อง
		3. การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ 4. เป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ที่จำเป็นในการปฏิบัติหน้าที่ตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านการสาธารณสุข 5. เป็นการเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย

โดยผู้บริหารและพนักงานของหน่วยงานที่รับผิดชอบสามารถอ้างอิงรายละเอียดเพิ่มเติมเกี่ยวกับเงื่อนไขดังกล่าวได้ใน *"คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)"* ทั้งนี้ ผู้บริหารและพนักงานของหน่วยงานที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมเหตุผลของการปฏิเสธคำร้องในทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล[100] ในทุกกรณีการปฏิเสธคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล[101]กำหนด

บริษัทฯ กำหนดให้มีการสอบทานและทบทวนกระบวนการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล[102] อย่างน้อยปีละ 1 ครั้ง เพื่อให้กระบวนการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคลมีความเหมาะสมและสอดคล้องกับกฎหมายและ/หรือการตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กรณีที่กฎหมายดังกล่าวมีการเปลี่ยนแปลงไป

[100] ทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคลถูกจัดเก็บเป็นแบบ centralized โดยมีการจำกัดสิทธิให้หน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและเปลี่ยนแปลงข้อมูลได้เฉพาะข้อมูลที่หน่วยงานของตนเองรับผิดชอบ สำหรับ DPO จะมีสิทธิในการเข้าถึงและเปลี่ยนแปลงข้อมูลที่รับผิดชอบโดยหน่วยงานที่มีหน้าที่รับผิดชอบต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตลอดเวลาของทุกหน่วยงาน

[101] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 (7)

[102] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน "คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)" หัวข้อที่ 6.2.8 "การสอบทานและทบทวนกระบวนการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล"

9. การกำกับดูแลหน่วยงานภายนอก

บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) มีหน้าที่ในการกำกับดูแลหน่วยงานภายนอก (Third Party) เพื่อให้มั่นใจได้ว่าหน่วยงานภายนอกที่มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ (Data Processor) หรือหน่วยงานภายนอกอื่นที่บริษัทฯ มีการเปิดเผยข้อมูลส่วนบุคคลให้มีมาตรการในการคุ้มครองดูแลข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม ดังนั้น ผู้บริหารและพนักงานในแต่ละหน่วยงาน ต้องดำเนินการกำกับดูแลหน่วยงานภายนอก ตามข้อกำหนดด้านกำกับดูแลหน่วยงานภายนอก (Third Party Oversight) ดังต่อไปนี้

9.1 การประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล

เมื่อหน่วยงานภายในบริษัทฯ ซึ่งได้แก่ผู้บริหารและพนักงานในแต่ละหน่วยงาน จำเป็นต้องใช้บริการหน่วยงานภายนอก (Third Party) ดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ หน่วยงานภายในที่รับผิดชอบเกี่ยวกับการประเมินหน่วยงานภายนอก[103] ต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว ทำการประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล (Third Party Assessment for Data Privacy Protection) ก่อนดำเนินการตามกระบวนการจัดซื้อจัดจ้างทั่วไป เพื่อให้มั่นใจได้ว่าผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว มีมาตรการในการคุ้มครองดูแลข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม ตลอดระยะเวลาที่เป็นคู่สัญญากับบริษัทฯ

โดยการจัดทำการประเมินนั้น ให้ผู้บริหารและพนักงานของหน่วยงานภายในที่รับผิดชอบเกี่ยวกับการประเมินฯ บังคับใช้กับกรณี ดังต่อไปนี้

1. ผู้ประมวลผลข้อมูลส่วนบุคคลที่มีสัญญาบริการร่วมกันกับบริษัทฯ อยู่แล้ว (Existing Data Processor) หรือกรณีจะทำสัญญาการประมวลผลข้อมูลส่วนบุคคลใหม่ (New Contract)
2. ผู้ประมวลผลข้อมูลส่วนบุคคลรายใหม่ที่บริษัทฯ จะทำสัญญาร่วมด้วย (New Data Processor)

โดยแนวปฏิบัติรอบระยะเวลาและเงื่อนไขในการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล ต้องเป็นไปตามข้อกำหนดของบริษัทฯ ซึ่งระบุไว้ใน *"คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)"* ซึ่งประกอบด้วย 5 หัวข้อการประเมิน ดังนี้

1. การประเมินด้านโครงสร้างและบทบาทหน้าที่ของหน่วยงานกำกับดูแลข้อมูลส่วนบุคคลของหน่วยงานภายนอก (Privacy Governance Structure and Roles & Responsibilities)
2. การประเมินกระบวนการบันทึกการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภายนอก (Record of Processing Activities)
3. การประเมินเรื่องมาตรการการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานภายนอก (Personal Data Security Policy)
4. การประเมินเรื่องกระบวนการ ขั้นตอนการปฏิบัติงาน และเทคโนโลยีที่หน่วยงานภายนอกนำมาใช้เพื่อการประมวลผลข้อมูลส่วนบุคคลให้แก่บริษัทฯ (Process, Procedures and Technology)
5. การประเมินเรื่องการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Laws) ของหน่วยงานภายนอกในการประมวลผลข้อมูลส่วนบุคคล

[103] หน่วยงานภายในที่รับผิดชอบเกี่ยวกับการประเมินหน่วยงานภายนอก ได้แก่ ฝ่ายบริหารการจัดหาพัสดุ (PO) และหน่วยงานที่เป็นเจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Process Owner) อ้างอิงรายละเอียดเพิ่มเติมใน "คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)"

ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่ผ่านเกณฑ์ที่บริษัทฯ กำหนด แต่หน่วยงานภายในมีความจำเป็นต้องใช้บริการผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว ผู้บริหารและพนักงานของหน่วยงานภายในที่รับผิดชอบเกี่ยวกับเกี่ยวกับการประเมินฯ ต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นดำเนินการพัฒนาปรับปรุงตามเงื่อนไขของบริษัทฯ และได้รับการอนุมัติให้ดำเนินการจากผู้มีอำนาจอนุมัติหรือกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลไม่ยินยอมดำเนินการพัฒนาปรับปรุงตามเงื่อนไขของบริษัทฯ ต้องได้รับการอนุมัติให้ดำเนินการจากผู้มีอำนาจอนุมัติ ตามข้อกำหนดของบริษัทฯ ซึ่งระบุไว้ใน *"คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)"* ก่อนดำเนินการตามกระบวนการจัดซื้อจัดจ้างทั่วไป

9.2 การจัดทำสัญญากับหน่วยงานภายนอก

บริษัทฯ กำหนดให้หน่วยงานภายในแต่ละหน่วยงาน ต้องจัดทำข้อตกลงหรือสัญญาดังต่อไปนี้ เป็นลายลักษณ์อักษร อย่างชัดเจนและเหมาะสม และลงนามร่วมกับหน่วยงานภายนอกที่มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ (Data Processor) หรือหน่วยงานภายนอกอื่นที่บริษัทฯ มีการเปิดเผยข้อมูลส่วนบุคคลไปให้

1. **ข้อตกลงหรือสัญญาประมวลผลข้อมูล** (Data Processing Agreement) กรณีที่บริษัทฯ จ้างหน่วยงานภายนอกดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ หรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคลให้กับบริษัทฯ นั้น (Data Processor) ซึ่งข้อตกลงหรือสัญญาประมวลผลข้อมูล (Data Processing Agreement) เป็นการตกลงร่วมกันระหว่างบริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลกับหน่วยงานภายนอก ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับเงื่อนไขในการประมวลผลข้อมูลส่วนบุคคล ซึ่งกำหนดให้ผู้ประมวลผลข้อมูลต้องดำเนินการประมวลผลข้อมูลตามคำสั่งของบริษัทฯ เท่านั้น
2. **ข้อตกลงหรือสัญญาแบ่งปันข้อมูล** (Data Sharing Agreement) กรณีที่บริษัทฯ มีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่น ซึ่งข้อตกลงหรือสัญญาแบ่งปันข้อมูล (Data Sharing Agreement) เป็นการตกลงร่วมกันกับคู่สัญญา เพื่อสนับสนุนการแบ่งปันข้อมูลส่วนบุคคลระหว่างกัน โดยต่างฝ่ายต่างมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และแต่ละฝ่ายจะประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันตามวัตถุประสงค์ภายใต้ข้อตกลงและเงื่อนไขของสัญญาเท่านั้น

ทั้งนี้ สัญญาทั้ง 2 ประเภท ต้องมีเนื้อหาครอบคลุมเรื่องดังต่อไปนี้ เป็นอย่างน้อย

1. บทบาทหน้าที่และความรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมและชัดเจน
2. มาตรการรักษาความมั่นคงปลอดภัยรวมถึงการรักษาความลับของข้อมูลส่วนบุคคล
3. การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น ในการเก็บรักษาไว้ตามวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล
4. การจำกัดไม่ให้มีการส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลอื่น
5. การแจ้งเตือนเมื่อมีการรั่วไหลหรือเกิดการละเมิดข้อมูลส่วนบุคคล

นอกจากนี้ หน่วยงานภายในแต่ละหน่วยงานที่มีสัญญาร่วมกับหน่วยงานภายนอก (Third Party) มีหน้าที่ในการทบทวนสัญญาที่จัดทำกับหน่วยงานภายนอกที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ว่ายังมีความชัดเจนและเหมาะสมกับลักษณะการประมวลผลข้อมูลส่วนบุคคลหรือไม่ หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้มีการ

เปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของบริษัทฯ ไปให้บุคคลอื่นนอกเหนือจากที่ระบุในสัญญาหรือบุคคลที่ไม่ได้รับความยินยอมหรือไม่

โดยบริษัทฯ กำหนดให้หน่วยงานภายในแต่ละหน่วยงาน ต้องดำเนินการทบทวนข้อตกลงหรือสัญญาประมวลผลข้อมูลและสัญญาจ้างงานหน่วยงานภายนอกตามรอบระยะเวลาที่เหมาะสม อย่างน้อยปีละ 1 ครั้ง หรือหลังจากผู้ประมวลผลข้อมูลส่วนบุคคลที่ใช้บริการอยู่ในปัจจุบันทำการประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล (Third Party Assessment for Data Privacy Protection) รอบใหม่ หากพิจารณาแล้วพบว่า ข้อตกลงหรือสัญญาที่เกี่ยวข้องดังกล่าว (ฉบับปัจจุบัน) จำเป็นต้องแก้ไขเพิ่มเติมเพื่อให้มีความชัดเจนและเหมาะสมมากขึ้นตามลักษณะ และพฤติการณ์ของการประมวลผลข้อมูลของผู้ประมวลผลข้อมูลส่วนบุคคลที่เปลี่ยนแปลงไป หน่วยงานภายในแต่ละหน่วยงานต้องดำเนินการปรับปรุงข้อตกลงหรือสัญญาดังกล่าวทันที

9.3 การตรวจสอบหรือการกำกับดูแลหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้ DPO / DPO Office และหน่วยงานอื่นที่เกี่ยวข้อง เช่น ฝ่ายตรวจสอบภายใน (IA) มีหน้าที่ในการตรวจสอบหรือการกำกับดูแลหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคลให้มีความน่าเชื่อถือ โดยต้องดำเนินการตามเกณฑ์และรอบระยะเวลาที่เหมาะสม เพื่อให้มั่นใจว่าหน่วยงานภายนอกสามารถปฏิบัติตามนโยบายและแนวปฏิบัติที่บริษัทฯ กำหนด และปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

10. การจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล

เหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล หมายถึง เหตุการณ์ที่มีการรั่วไหลหรือละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และส่งผลให้เกิดการประมวลผล เข้าถึง เปิดเผย ทำสำเนา เปลี่ยนแปลง เก็บ ทำซ้ำ แสดง หรือจำหน่ายข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย หรือทำให้เกิดการสูญหาย ทำลาย เปลี่ยนแปลง หรือเสียหายต่อข้อมูลส่วนบุคคลโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย

ตัวอย่างของเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล ที่ทำให้เกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ได้แก่

1. เหตุละเมิดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (IT) เช่น ภัยคุกคามด้านระบบคอมพิวเตอร์ (Cyber Attack) เครื่องคอมพิวเตอร์เสียหาย สูญหาย ถูกทำลาย หรือไม่สามารถใช้การได้[104]
2. เหตุละเมิดที่ไม่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (Non-IT) เช่น เอกสารสำคัญที่จัดเก็บข้อมูลส่วนบุคคล สูญหายหรือถูกขโมย การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจ การลักลอบนำข้อมูลส่วนบุคคลที่บริษัทฯ จัดเก็บไปเปิดเผยหรือนำไปใช้ประโยชน์อื่นโดยที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม รวมถึงการเกิดเหตุสุดวิสัย หรือภัยพิบัติทางธรรมชาติ เช่น ไฟไหม้ น้ำท่วม เป็นต้น

บริษัทฯ กำหนดให้ผู้บริหารและพนักงานทุกหน่วยงานมีหน้าที่รับผิดชอบต่อการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล โดยต้องจัดเตรียมกลไกหรือกระบวนการเพื่อใช้สำหรับรองรับการบริหารจัดการเหตุละเมิดและการ

[104] อ้างอิงตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Security Policy)

รั่วไหลของข้อมูลส่วนบุคคล ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด และกำหนดให้ผู้บริหารและพนักงานทุกคนต้องปฏิบัติตามแนวปฏิบัติในการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลที่บริษัทฯ กำหนด[105] ไว้อย่างเคร่งครัด เพื่อให้เหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลได้รับการจัดการอย่างเหมาะสมและเพื่อลดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลให้ได้มากที่สุด

บริษัทฯ กำหนดให้กลไกหรือกระบวนการเพื่อใช้สำหรับการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลที่ผู้บริหารและพนักงานทุกหน่วยงานต้องจัดเตรียมนั้น ต้องมีขั้นตอนการจัดการครอบคลุม ตั้งแต่การตรวจพบเหตุการณ์ผิดปกติ เหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล การดำเนินการสืบสวน การวิเคราะห์หาสาเหตุ การประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล การจัดทำแผนการแก้ไขและแนวทางในการเยียวยา การดำเนินการแก้ไขเหตุละเมิด การแจ้งเหตุละเมิด การติดตามผลการแก้ไขเหตุละเมิด รวมถึงการบันทึกข้อมูลในทะเบียนเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Incident and Breach Log) และการปิดสถานะของเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล เมื่อดำเนินการแก้ไขแล้วเสร็จ

บริษัทฯ กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer หรือ DPO) ดำเนินการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง[106] นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลอย่างมาก และหากกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลอื่นที่ได้รับมอบหมายโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลรับทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

บริษัทฯ กำหนดให้มีการสอบทานและทบทวนกระบวนการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล[107]อย่างน้อยปีละ 1 ครั้ง เพื่อให้กระบวนการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลมีประสิทธิภาพ เหมาะสม และสอดคล้องกับกฎหมายและ/หรือการตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กรณีที่กฎหมายดังกล่าวมีการเปลี่ยนแปลงไป

11. การกำกับดูแลการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ กำหนดให้มีการติดตามตรวจสอบการดำเนินงานเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่การเก็บรวบรวม ใช้ เปิดเผย ตลอดจนการเก็บรักษาและการทำลายข้อมูลส่วนบุคคลของบริษัทฯ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าผู้บริหารและพนักงานของบริษัทฯ ปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ซึ่งเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยหน้าที่การติดตามตรวจสอบดังกล่าวอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer หรือ DPO) โดยสามารถอ้างอิงรายละเอียดเพิ่มเติมได้ใน *“กฎบัตรการคุ้มครองข้อมูลส่วนบุคคล”*

[105] สามารถอ้างอิงรายละเอียดเพิ่มเติมใน “คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)”

[106] อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ระบุว่า แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

[107] สามารถอ้างอิงรายละเอียดแนวปฏิบัติเกี่ยวกับ การสอบทานและทบทวนกระบวนการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคลอยู่ภายใต้ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer หรือ DPO) ใน “คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)” หัวข้อการสอบทานและทบทวนกระบวนการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล

ทั้งนี้ ในกรณีที่พบประเด็น Non-compliance จากการติดตามตรวจสอบ DPO จะจัดทำรายงานสรุปผลการตรวจสอบและรายงานให้ผู้บริหารระดับสูงของหน่วยงานที่พบประเด็น Non-compliance ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ และคณะกรรมการบริหารและจัดการบริษัทได้รับทราบ และติดตามความคืบหน้าการปรับปรุงแก้ไขในการรายงานครั้งต่อไป

อย่างไรก็ตาม ในกรณีที่ประเด็น Non-compliance นั้นมีความเสี่ยงสูง DPO จะรายงานและติดตามความคืบหน้าโดยเร็วที่สุดตามคำสั่งของประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่และคณะกรรมการบริหารและจัดการบริษัท เพื่อดำเนินการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและ/หรือเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อไป[108]

12. นโยบายและคู่มือแนวปฏิบัติอื่นที่เกี่ยวข้อง

เพื่อให้ผู้บริหารและพนักงานสามารถปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล นโยบายคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ บริษัทฯ จึงได้สรุปความเชื่อมโยงระหว่างแนวปฏิบัติฉบับนี้กับนโยบายและคู่มือแนวปฏิบัติอื่นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยแบ่งแยกตามหมวดหมู่ ดังปรากฏในตารางด้านล่างนี้

ลำดับ	ชื่อนโยบาย / คู่มือแนวปฏิบัติ	เรื่องที่เกี่ยวข้อง
1	กฎบัตรการคุ้มครองข้อมูลส่วนบุคคล	ข้อ 2.3 หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 11 การกำกับดูแลการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล
2	นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Security Policy)	ข้อ 7.1.3.1 การจัดเก็บข้อมูลส่วนบุคคล ข้อ 10 การจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล
3	คู่มือการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Data Protection Impact Assessment หรือ DPIA)	ข้อ 2.1 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ข้อ 4.1.3 การคำนึงถึงสิทธิความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบ (Privacy by Design)
4	คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Third Party Assessment – Data Privacy Protection)	ข้อ 2.1 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ข้อ 9.1 การประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล
5	คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management)	ข้อ 2.1 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ข้อ 2.2 หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล

[108] อ้างอิงตามกฎบัตรการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อนโยบาย / คู่มือแนวปฏิบัติ	เรื่องที่เกี่ยวข้อง
		ข้อ 6.3.2 การถอนความยินยอม ข้อ 7.1.4 การทำลายข้อมูลส่วนบุคคล ข้อ 7.2 การบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) ข้อ 8 การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล
6	คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)	ข้อ 2.1 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล ข้อ 10. การจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล
7	ประกาศ เรื่อง การบันทึกข้อมูลส่วนบุคคลผ่านกล้องโทรทัศน์วงจรปิด (Closed-circuit Television (CCTV) Privacy Notice)	ข้อ 5.5 ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate interest)

13. บทลงโทษ

กรณีที่บริษัทฯ พบว่า ผู้บริหารและพนักงานกระทำผิดโดยการไม่ปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ รวมถึงกฎหมายที่มีผลบังคับใช้กับบริษัทฯ ไม่ว่าโดยจงใจ หรือประมาทเลินเล่อ ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลโดยการฝ่าฝืนข้อบังคับเกี่ยวกับการทำงานและคำสั่งของบริษัทฯ ซึ่งผู้บริหารและพนักงานจะได้รับโทษทางวินัยตามที่บริษัทฯ กำหนด

ทั้งนี้ หากการกระทำดังกล่าวเป็นการดำเนินการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบหรือโดยฝ่าฝืนข้อกำหนดหรือข้อบังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้บริหารและพนักงานอาจถูกดำเนินคดีตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

14. การทบทวนนโยบายและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล

นโยบายและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลจะได้รับการทบทวนและปรับปรุงอย่างน้อยทุก 2 ปี หรือเมื่อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมีการปรับเปลี่ยนหรือแก้ไขเพิ่มเติมข้อกำหนด เพื่อให้สามารถใช้บังคับได้อย่างเหมาะสมกับสถานการณ์และสอดคล้องกับแนวปฏิบัติหรือข้อบังคับทางกฎหมายที่เปลี่ยนแปลงไป

ทั้งนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ในการปรับปรุงและทบทวนนโยบายและแนวปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ให้เป็นไปอย่างเพียงพอและเหมาะสม โดยได้รับการสนับสนุนจาก

1. หน่วยงานกำกับการปฏิบัติงาน (Compliance) หรือหน่วยงานควบคุมภายใน (Internal Control)
2. คณะทำงานสนับสนุนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Office) ซึ่งประกอบไปด้วยฝ่ายบริหารทรัพยากรบุคคลและพัฒนาองค์กร (HR), ฝ่ายยุทธศาสตร์และความเสี่ยงองค์กร (SR), ฝ่ายตรวจสอบภายใน (IA) และสำนักกฎหมายและเลขานุการบริษัท (LC)