สรุปบทเรียนจากการพัฒนาความรู้ รอบที่ 1 ประจำปี 2568
ของ นางสาวสมจินต์ วานิชเสถียร
เรื่อง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

PDPA พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บรรยายโดย ผศ.ดร.ประพันธ์พงษ์ ขำอ่อน

1. ที่มาและเจตนา และการบังคับใช้กฎหมาย

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล และเยียวยาเจ้าของข้อมูลส่วนบุคคล จากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล เป็นกฎหมายที่บังคับใช้กับทั้งหน่วยงานภาครัฐ และเอกชน

ที่มาและเจตนาในการคุ้มครองข้อมูลส่วนบุคคล

1.1 สร้างความเชื่อมั่น (Trust) สร้างความเชื่อมั่นให้กับเจ้าของข้อมูลส่วนบุคคลในการเข้ารับบริการหรือดำเนินกิจกรรมกับหน่วยงานที่ทำการใช้ข้อมูลส่วนบุคคล ว่าหน่วยงานจะมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน

1.2 ยกระดับการธรรมาภิบาลข้อมูล (Better data governance) สร้างหน้าที่ให้กับหน่วยงานทั้งภาครัฐและเอกชนในการสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นปัจจัยสำคัญในการยกระดับการธรรมาภิบาลข้อมูล

1.3 ยกระดับสู่มาตรฐานสากล (Connecting with global standards) ยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎเกณฑ์และมาตรฐานสากล เพื่อสร้างความเชื่อมั่นให้กับหน่วยงานในต่างประเทศในการดำเนินการค้าและการลงทุนกับประเทศไทย

2. นิยามเจ้าของข้อมูลส่วนบุคคล/ผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล (Processing) คือ การดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการใช้ เก็บรวบรวม จัดเก็บ ลบ ทำลาย เปิดเผย เชื่อมโยง เปลี่ยนแปลง ส่งผ่าน หรือ Update ข้อมูล

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลทั้งหมด

ผู้ที่เกี่ยวข้องใน PDPA ได้แก่

2.1 หน่วยงานผู้กำกับดูแล (Data protection authority)

2.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) คือ บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2.3 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data processor) คือ บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

2.4 เจ้าของข้อมูลส่วนบุคคล (Data subject) คือ บุคคลผู้ซึ่งข้อมูลส่วนบุคคลถูกประมวลผล (เก็บรวบรวม ใช้ หรือเปิดเผย)

3. ข้อมูลส่วนบุคคล (นิยาม/ประเภท)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ได้แก่

ชื่อ-นามสกุล เพศ อายุ วันเดือนปีเกิด สถานภาพการสมรส ที่อยู่ อีเมลที่ระบุตัวตนได้ หมายเลขไอพี และเลขที่หนังสือเดินทาง

ข้อมูลอ่อนไหว (Sensitive data) ตามมาตรา 26 ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา ปรัชญา พฤติกรรมทางเพศ ข้อมูลสุขภาพ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ความพิการ ข้อมูลสหภาพแรงงาน และประวัติอาชญากรรม

ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย การเปิดเผยข้อมูลที่อ่อนไหวที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย ทำให้ผู้กระทำผิดรับโทษ ดังนี้

3.1 โทษปรับหน่วยงาน สูงสุด 5 ล้านบาท (ม.84) ซึ่งหน่วยงานสามารถไล่เบี้ยกับพนักงานที่ทำผิดได้

3.2 โทษทางแพ่ง โดยที่ผู้เสียหายสามารถเรียกร้องค่าเสียหายได้ไม่เกิน 2 เท่าของความเสียหายจริง

3.3 โทษอาญา จำคุกไม่เกิน 6 เดือนหรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ (โทษสำหรับบุคคลและ/หรือนิติบุคคลที่เปิดเผยข้อมูล)

4. หลักการการคุ้มครองข้อมูลส่วนบุคคล

4.1 หลักการของ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

1) Lawful processing and transparency มีความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลและมีความโปร่งใส

2) Necessity and Purpose Limitation ใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์และเท่าที่จำเป็น

3) Data Accuracy ต้องทำข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน

4) Limitation of Storage มีระยะเวลาในการเก็บข้อมูลส่วนบุคคลที่แน่นอน

5) Security มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

6) เคารพสิทธิของ Data Subject ดำเนินการตามคำร้องขอของ Data Subject ตามขอบเขตที่กฎหมายกำหนด

4.2 ฐานการประมวลผล (Lawful Basis) สำหรับการประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

1) ฐานการขอความยินยอม (Consent)

2) ฐานระงับอันตรายต่อชีวิต (Vital Interest)

3) ฐานการจัดทำเอกสารประวัติศาสตร์เพื่อประโยชน์สาธารณะหรือการวิจัย (Historical Archive & Research)

4) ฐานจำเป็นเพื่อปฏิบัติตามสัญญา (Contract)

5) ฐานปฏิบัติตามกฎหมาย (Legal Obligation)

6) ฐานผลประโยชน์อันชอบธรรมที่ไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject (Legitimate Interest)

7) ฐานภารกิจรัฐหรือฐานเพื่อประโยชน์สาธารณะ (Public Task)

4.3 ฐานการประมวลผล (Lawful Basis) สำหรับการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

1) ฐานการขอความยินยอมโดยชัดแจ้ง (Explicit Consent)

2) ฐานการระงับอันตรายต่อชีวิต (Vital Interest)

3) ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน (Special Objectives)

4) ฐานจำเป็นเพื่อปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์ (Medical Contract)

5) ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Claim of Legal Rights)

6) ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการแพทย์ ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย และประโยชน์สาธารณะที่สำคัญ (Legal Obligations with Specific Purposes)

7) ฐานการเก็บรวบรวมประวัติอาชญากรรมภายใต้การควบคุมของหน่วยงานที่มีอำนาจด้านกฎหมาย (Criminal Records)

5. หน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่ของ Data Controller ตามกฎหมาย PDPA

5.1 แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล Privacy Notice (ม.23)

5.2 มีความชอบธรรมในการประมวลผล Lawful basis (ม.24, 26)

5.3 เก็บ ใช้ เปิดเผยเท่าที่จำเป็นและตามวัตถุประสงค์ Purpose Limitation (ม.22, 27)

5.4 ป้องกันมิให้บุคคลหรือองค์กรอื่นที่รับข้อมูลจาก data others from unlawful use or disclosure (ม.37(2))

5.5 ทำข้อมูลส่วนบุคคลให้ถูกต้อง Data Accuracy (ม.35)

5.6 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม Appropriate Security (ม.37(1))

5.7 แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบภายใน 72 ชั่วโมง Breach Notification (ม.37(4))

5.8 มีการตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็น และมีการจัดการสิทธิเจ้าของข้อมูลส่วนบุคคล Data Check and Data Subject Right Management (ม.37(3))

5.9 ทำบันทึกรายการกิจกรรมที่ใช้ข้อมูลส่วนบุคคล Records of Processing Activity (RoPA) (ม.39)

5.10 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)

Data Controller ต้องบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคลของหน่วยงานเพื่อให้เจ้าของข้อมูลส่วนบุคคล หรือ สคส. ตรวจสอบได้ โดยในแต่ละกิจกรรมต้องมีการบันทึกรายการเหล่านี้เป็นอย่างน้อย ได้แก่ ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม วัตถุประสงค์ของการเก็บรวบรวม ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ระยะเวลาการเก็บข้อมูลส่วนบุคคล สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคลให้บุคคลภายนอกหรือองค์กรภายนอก การปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรการรักษาความมั่นคงปลอดภัย

6. หน้าที่ตามกฎหมายของผู้ประมวลผลข้อมูลส่วนบุคคล

6.1 หน้าที่ของ Data Processor ตามกฎหมาย PDPA

1) ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล

2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

3) แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ data controller ทราบ

4) ทำบันทึกรายการการประมวลผลข้อมูล (RoPA) (ถ้าเป็นไปตามเกณฑ์ต้องจัดทำ)

5) แต่งตั้ง DPO (ถ้าเป็นไปตามเกณฑ์ต้องแต่งตั้ง)

6.2 แนวทางการควบคุมเพื่อป้องกันไม่ให้บุคคล/นิติบุคคลที่รับข้อมูลส่วนบุคคล ดำเนินการใช้หรือเปิดเผยข้อมูลโดยไม่มีความมั่นคงปลอดภัย

1) สร้างมาตรการความมั่นคงปลอดภัย โดยการเข้ารหัสไฟล์ก่อนส่ง มาตรการนี้ใช้ทั้งกับการส่งข้อมูลส่วนบุคคลให้กับองค์กรภายนอก (เช่น เป็นบริษัทที่ตามภารกิจแล้วต้องมีการรับ-ส่งข้อมูล) และการส่งข้อมูลให้กับ Data Processor

2) ทำสัญญาประมวลผลข้อมูลส่วนบุคคล เพื่อกำกับดูแลให้ผู้ประมวลผลข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลที่เป็นไปตามมาตรฐาน PDPA

7. สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)

7.1 สิทธิในการเพิกถอนความยินยอมที่เคยให้ไว้เมื่อใดก็ได้ (ม.19)

7.2 สิทธิในการขอแก้ไขให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification) (ม.35)

7.3 สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access) (ม.30)

หลักเกณฑ์การใช้สิทธิ

1) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล

2) เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม

3) ในกรณีที่เจ้าของข้อมูลมีคำขอ และ DC ไม่อาจปฏิเสธคำขอได้ DC ต้องดำเนินการตามคำขอโดยไม่ชักช้า (ไม่เกิน 30 วันนับแต่ได้รับคำขอ)

เหตุในการปฏิเสธคำขอ

1) ต้องทำตามกฎหมาย เช่น กรณีที่มีกฎหมายห้ามเจ้าของข้อมูลเข้าถึงข้อมูลส่วนตัวในบางกรณี

2) ต้องทำตามคำสั่งศาล

3) คำขอก่อให้เกิดความเสียหายและกระทบต่อสิทธิเสรีภาพของบุคคลอื่น เช่น การเข้าถึงข้อมูลนั้นทำให้ล่วงรู้ความลับของผู้อื่นหรือมีความเสี่ยงในการละเมิดข้อมูลส่วนบุคคลของผู้อื่น

7.4 สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure) (ม.33)

หลักเกณฑ์การใช้สิทธิ

1) เมื่อข้อมูลไม่จำเป็นสำหรับวัตถุประสงค์ในการเก็บรวบรวมและใช้อีกต่อไป หรือเจ้าของข้อมูลไม่ได้ใช้บริการที่มีการประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม

3) เมื่อข้อมูลส่วนบุคคลได้รับการประมวลผลโดยไม่ชอบด้วยกฎหมาย

เหตุในการปฏิเสธคำขอ

1) เก็บรักษาไว้เพื่อวัตถุประสงค์การใช้เสรีภาพในการแสดงความคิดเห็น เช่น กรณีที่กฎหมายกำหนดให้จัดเก็บข้อมูลยืนยันตัวตนของผู้แสดงความคิดเห็นในสื่อ Social Media

2) เก็บรักษาไว้เพื่อวัตถุประสงค์ในการศึกษาวิจัยหรือสถิติ/ป้องกันหรือระงับอันตรายต่อชีวิต/ปฏิบัติตามกฎหมายทางการแพทย์และสาธารณสุข เช่น การให้บริการด้านสุขภาพ การป้องกันโรคติดต่อ เช่น มีระเบียบการทรวงสาธารณสุขกำหนดให้เก็บข้อมูลเวชระเบียนคนไข้ไม่ต่ำกว่า 5 ปี

3) เก็บรักษาไว้เพื่อวัตถุประสงค์ในการก่อตั้งสิทธิตามกฎหมาย หรือปฏิบัติตามกฎหมาย

7.5 สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict) (ม.34)

7.6 สิทธิขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object) (ม.32)

หลักเกณฑ์การใช้สิทธิ

1) เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการใช้ข้อมูลขององค์กรได้

2) เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการใช้ข้อมูลเพื่อการตลาดแบบตรง

3) เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการใช้ข้อมูลเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

เหตุในการปฏิเสธคำขอ

1) DC แสดงให้เห็นเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า เช่น กรณีการระงับอัตรายต่อชีวิต หรือจำเป็นเพื่อปฏิบัติภารกิจเพื่อประโยชน์สาธารณะ

2) เป็นการก่อตั้งสิทธิเรียกร้องตามกฎหมาย หรือการปฏิบัติตามกฎหมาย

3) ความจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ เช่น การเก็บข้อมูลคดีเมาแล้วขับ

7.7 สิทธิในการขอให้โอนข้อมูลส่วนบุคคลไปยัง Data Controller อื่นด้วยวิธีการอัตโนมัติ หรือขอรับข้อมูลที่โอนไปให้ Data Controller อื่น (Right to data portability) (ม.31)

8. ความรับผิดชอบ

8.1 การลงโทษผู้ไม่ปฏิบัติตาม

1) ความรับผิดทางแพ่ง (ม.77-78)

2) โทษทางอาญา (ม.79-81) โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท)

3) การปรับทางปกครอง (ม.82-90) โทษปรับ 1 - 5 ล้านบาท

8.2 ข้อพิจารณาในการลงโทษปรับทางปกครองสำหรับผู้ทำความผิด

เมื่อกฎหมายดูมาตรการขององค์กรเป็นหลักว่ามีการดำเนินการเพื่อไม่ให้ผิด PDPA หรือไม่ ดังนั้น หน่วยงานต้องจัดให้มีมาตรการตามที่กฎหมาย มาตรการที่ สคส. จะนำมาพิจารณาโทษปรับปกครองดูจากพฤติกรรมของหน่วยงาน (ม.8 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์การพิจารณาออกคำสั่งลงโทษทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565) ในด้านต่อไปนี้

1) เจตนาหรือความจงใจในการกระทำผิด

2) ความระมัดระวัง

3) มูลค่าความเสียหายและความร้ายแรงของเหตุ

4) ระดับความรับผิดชอบและมาตรฐานด้าน PDPA ขณะที่เหตุเกิด

5) การดำเนินการตามแนวปฏิบัติทางธุรกิจ หรือมาตรฐานด้านความมั่นคงปลอดภัย

6) การเยียวยาและบรรเทาเหตุขณะที่เกิดขึ้น

9. สิ่งที่องค์กรต้องเตรียมตัว

9.1 Collection

1) แจ้งเจ้าของข้อมูลส่วนบุคคลว่าวัตถุประสงค์ในการเก็บ/ใช้คืออะไร โดยแจ้งผ่านเอกสารการแจ้งการประมวลผล (Privacy Notice)

9.2 Usage

1) กำหนดแนวทาง/นโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (standard operating procedure)

2) บันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บ/ใช้ (Records of Processing. Activity: ROPA)

9.3 Disclosure/Transfer

1) ทำสัญญา/ข้อตกลงกับบุคคลภายนอกหรือทำ data processing agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมาย

2) ในกรณีโอนข้อมูลไปต่างประเทศ ดูว่าเข้าเงื่อนไขตาม PDPA หรือไม่ (เช่น ดูว่าประเทศนั้นมีมาตรฐานเพียงพอ การทำสัญญากับหน่วยงาน หรือการขอความยินยอม Data Subject ฯลฯ)

9.4 Storage/Disposal

1) กำหนดแนวทางด้านมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Security) เช่น access control, security assessment, security policy

2) กำหนดนโยบายระยะเวลาเก็บข้อมูลและการทำลายเอกสารที่มีข้อมูลส่วนบุคคล

9.5 Governance

1) มีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล (data subject right)

2) มีกระบวนการแจ้งเหตุ (Breach notification protocol)

3) Data protection officer (DPO) ที่ให้คำปรึกษากับองค์กร และดูแลการดำเนินการให้เป็นไปตามกฎหมาย

4) อบรม (Training) ให้พนักงานมีความเข้าใจ

10. ข้อแนะนำ ข้อพึงระวัง และสรุป

10.1 เป้าหมายของการทำตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1) ไม่ละเมิด (กฎหมายดูมาตรการขององค์กรเป็นสำคัญ)

2) ไม่โดนปรับ (กฎหมายดูมาตรการขององค์กรเป็นสำคัญ)

3) สร้างความเชื่อมั่นให้เจ้าของข้อมูลส่วนบุคคล

4) สร้างฐานให้นำ IT Tech % Big Data มาใช้ได้อย่างมั่นใจ

5) สร้างความได้เปรียบทางการแข่งขัน

10.2 ความรับผิดและโทษของ PDPA ต่อองค์กร

1) โทษปรับปกครองสูงสุด 5 ล้านบาท

2) จ่ายค่าเสียหายตามจริง แต่ศาลอาจสั่งให้จ่ายถึง 2 เท่าของค่าเสียหายตามจริงได้

3) โทษจำคุกสูงสุด 1 ปี (เฉพาะความผิดที่เป็นโทษอาญา)

4) ผู้ต้องรับผิดชอบคือ องค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

5) เมื่อองค์กรรับผิดแล้ว อาจใช้สิทธิทางกฎหมายไล่เบี้ยพนักงานหรือลูกจ้างที่ทำการละเมิดข้อมูลส่วนบุคคลทั้ง ๆ ที่องค์กรได้มีนโนบายกำกับดูแลไว้เป็นอย่างดีแล้วได้