สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

คู่มือ PDPA
สำหรับผู้ประกอบการ SMEs

โดย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เฟสบุ๊ค: https://www.facebook.com/pdpc.th
โทรศัพท์: 1111

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

คู่มือ PDPA
สำหรับผู้ประกอบการ SMEs

ฉบับ 21 มิถุนายน 2565

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

Call Center : 1111 หรือ 02-142-1033 หรือ 02-141-6993

Facebook: https://www.facebook.com/pdpc.th

สารบัญ

บทที่ 1 ทำความเข้าใจเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล 1

บทที่ 2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในกิจการขนาดเล็ก 3

1. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล 3
2. ข้อยกเว้นของผู้ประกอบการซึ่งเป็นกิจการขนาดเล็ก 8

บทที่ 3 การจัดทำบันทึกรายการ 11

1. วัตถุประสงค์ของการจัดทำบันทึกรายการและบันทึกรายการของกิจกรรม การประมวลผลข้อมูลส่วนบุคคล 11
2. การจัดทำบันทึกรายการสำหรับผู้ควบคุมข้อมูลส่วนบุคคล 11
3. การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล 14

บทที่ 4 การจัดการมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล 17

1. วัตถุประสงค์และความจำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 17
2. แนวทางการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคล 17
3. การทบทวนมาตรการรักษาความมั่นคงปลอดภัยในปัจจุบัน 19

ภาคผนวก

ก. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการ ของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

ข. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการ ในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ค. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

บทที่ 1 ทำความเข้าใจเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่มีวัตถุประสงค์เพื่อการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนในฐานะเจ้าของข้อมูลส่วนบุคคลโดยกำหนดหน้าที่และความรับผิดชอบให้องค์กรปฏิบัติตามกฎหมาย บทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีลักษณะพิเศษแตกต่างจากกฎหมายฉบับอื่น กล่าวคือ ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่บทบัญญัติส่งเสริมการสร้างความตระหนักรู้ และการทบทวนกระบวนการทำงาน เพื่อให้การกระทำใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวภายใต้หลักการของรัฐธรรมนูญ

> *“กฎหมายไม่ได้มุ่งสร้างภาระในการเก็บและใช้ข้อมูล แต่ต้องการให้มีกระบวนการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสม ปลอดภัย โดยคำนึงถึงสิทธิความเป็นส่วนตัวของบุคคลเพื่อให้ได้รับผลกระทบน้อยที่สุด”*

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัว หรือกิจกรรมในครอบครัว ได้รับการยกเว้น ทำให้ไม่ต้องปฏิบัติตามกฎหมายนี้

กฎหมายใช้บังคับกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจ องค์กรไม่แสวงหาผลกำไรและหน่วยงานของรัฐ โดยไม่จำกัดว่ากิจกรรมดังกล่าวจะเกิดขึ้นในรูปแบบกระดาษหรือในระบบดิจิทัล อย่างไรก็ตาม กฎหมายไม่ได้ห้ามประมวลผลข้อมูลส่วนบุคคลโดยสิ้นเชิง นั่นหมายความว่าผู้ประกอบการยังสามารถดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ได้เช่นเดียวกับที่เคยปฏิบัติตราบเท่าที่ไม่ขัดต่อเงื่อนไขที่กฎหมายกำหนด

ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลนี้กำหนดให้มีผู้เกี่ยวข้อง 3 บทบาท ได้แก่

- **เจ้าของข้อมูลส่วนบุคคล** (Data Subject) คือ ผู้มีสิทธิตามกฎหมาย ซึ่งข้อมูลนั้นบ่งชี้ไปถึงบุคคลดังกล่าวไม่ว่าทางตรงหรือทางอ้อม
- **ผู้ควบคุมข้อมูลส่วนบุคคล** (Data Controller) คือ บุคคลหรือนิติบุคคล ซึ่งมีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **ผู้ประมวลผลข้อมูลส่วนบุคคล** (Data Processor) คือ บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ บริษัท ห้างหุ้นส่วน ทั้งเป็นนิติบุคคลและไม่เป็นนิติบุคคล หรือผู้ประกอบธุรกิจฟรีแลนซ์ ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือพนักงาน

ตัวอย่าง ร้านกาแฟเป็นห้างหุ้นส่วนนิติบุคคลมีการเก็บรวบรวมข้อมูลลูกค้าเพื่อใช้ทำระบบสมาชิก

หน้าที่ส่วนใหญ่ตามกฎหมายนี้กำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล ได้แก่ บริษัท ห้างหุ้นส่วนทั้งเป็นนิติบุคคลและไม่เป็นนิติบุคคล และผู้ประกอบธุรกิจฟรีแลนซ์ที่รับจ้างหรือให้บริการแก่ผู้ควบคุมข้อมูลส่วนบุคคลทำกิจกรรมที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ตัวอย่าง ธุรกิจร้านค้าอาจจ้างบริษัทอื่นให้จัดการข้อมูลสั่งซื้อสินค้าหรือดูแลเฟซบุ๊กเพจของร้าน ซึ่งต้องมีการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของลูกค้า

บทที่ 2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ในกิจการขนาดเล็ก

ในปัจจุบัน “ข้อมูลส่วนบุคคล” ถือว่ามีความสำคัญอย่างมาก เนื่องจากเป็นข้อมูลที่ทั้งสามารถระบุตัวตนของผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้และในทางเศรษฐกิจยังมีประโยชน์และมูลค่าที่สูง หากใช้ในการประกอบธุรกิจประเภทต่างๆ ดังนั้น เมื่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้แล้วเมื่อวันที่ 1 มิถุนายน 2565 จึงทำให้ผู้ประกอบการที่อยู่ในฐานะของ “**ผู้ควบคุมข้อมูลส่วนบุคคล**” หรือ **“Data Controller”** มีหน้าที่ที่จะต้องปฏิบัติตามกฎหมาย เช่น การแจ้งรายละเอียดตามที่กฎหมายกำหนดให้กับลูกค้าหรือพนักงานทราบ การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐาน รวมถึงการจัดทำบันทึกรายการ เป็นต้น เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

1. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเมื่อมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตัวอย่างเช่น การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลส่วนบุคคลทราบ การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม หรือการต้องแจ้งเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลหากเกิดการรั่วไหลหรือมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น รวมถึงยังมีหน้าที่จะต้องจัดทำบันทึกรายการ โดยกฎหมายกำหนดหน้าที่เอาไว้ดังนี้

1.1 การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

- วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และฐานอำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคล
- การปฏิบัติตามกฎหมาย สัญญา หรือการแจ้งรายละเอียดประโยชน์โดยชอบด้วยกฎหมาย
- ประเภทของข้อมูลส่วนบุคคลและระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล
- ประเภทของผู้รับข้อมูล ในกรณีที่มีการส่งข้อมูลส่วนบุคคลให้กับบุคคลที่สาม
- แหล่งที่มาของข้อมูลส่วนบุคคล (กรณีเก็บรวบรวมข้อมูลมาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง)
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล

การแจ้งรายละเอียดของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลข้างต้นอาจอยู่ในรูปแบบของ “ประกาศการคุ้มครองข้อมูลส่วนบุคคล” หรือ “privacy notice” ซึ่งกฎหมายไม่ได้กำหนดมีรูปแบบตายตัว อาจทำได้หลายวิธี ทั้งการทำเป็นหนังสือลายลักษณ์อักษร ทางวาจา หรือสื่ออิเล็กทรอนิกส์ เช่น ข้อความ SMS อีเมล เป็นต้น โดยอาจแจ้งข้อมูลเบื้องต้นแบบสั้นและจัดทำเป็นลิงก์หรือ QR Code เชื่อมโยง

ไปเว็บไซต์เพื่อแจ้งรายละเอียดที่ครบถ้วนตามที่กฎหมายกำหนดอีกชั้นหนึ่ง (Layered Approach) ทั้งนี้ ผู้ประกอบการสามารถปรับแก้ตัวอย่างประกาศด้านล่างนี้ให้สอดคล้องกับกิจกรรมและรูปแบบการใช้งานได้ โดยวิธีการแจ้งควรจะแจ้ง ณ จุดที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลในแต่ละกิจกรรม ตัวอย่างเช่น การติดประกาศเกาการคุ้มครองข้อมูลส่วนบุคคลเฉพาะกิจกรรมการให้บริการลูกค้าไว้ที่จุดให้บริการ

ตัวอย่างประกาศการคุ้มครองข้อมูลส่วนบุคคล ณ จุดให้บริการ

ประกาศการคุ้มครองข้อมูลส่วนบุคคล
(Privacy Notice)

บริษัทมีการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อประโยชน์ในการให้บริการ โดยบริษัทดำเนินการประมวลผลข้อมูลของท่านด้วยความระมัดระวัง และตระหนักถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลของท่านด้วยมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่น้อยกว่าระดับที่กฎหมายกำหนด

กรณีมีข้อสงสัยเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลติดต่อได้ทางช่องทาง

- **Call Center XX-XXX**
- **คุณไฉไล ไฉไลมาก เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

[QR code
– ประกาศการคุ้มครองข้อมูลส่วนบุคคลฉบับเต็ม]

ในกรณีของการจ้างพนักงานอาจเพิ่มเรื่องประกาศการคุ้มครองข้อมูลส่วนบุคคลอาจจะระบุไว้ในส่วนใดส่วนหนึ่งของสัญญาจ้างงานก็ได้ เช่น ในส่วนท้ายของสัญญาจ้างงาน เป็นต้น

ตัวอย่างประกาศการคุ้มครองข้อมูลส่วนบุคคลในข้อสัญญาจ้างงาน

การจัดการข้อมูลส่วนบุคคล

ภายใต้ข้อสัญญาฉบับนี้ “ผู้ว่าจ้าง” ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะทำการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงาน ได้แก่ ข้อมูลเพื่อประกอบการทำสัญญา ซึ่งหมายความรวมถึงข้อมูลที่ผู้ว่าจ้างได้รับจากพนักงานในขั้นตอนการพิจารณาคุณสมบัติก่อนเข้าทำสัญญา ข้อมูลที่เกี่ยวข้องกับการปฏิบัติตามสัญญา ตลอดจนการจัดการสิทธิสวัสดิการของพนักงาน และ/หรือข้อมูลอื่นใดที่บริษัทได้รับจากพนักงานในระหว่างปฏิบัติงานให้กับผู้ว่าจ้าง โดยผู้ว่าจ้างจัดการข้อมูลของพนักงานด้วยความระมัดระวัง และตระหนักถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลของท่านด้วยมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่น้อยกว่าระดับที่กฎหมายกำหนด และเมื่อความสัมพันธ์ตามสัญญาสิ้นสุดลง บริษัทจะทำการลบข้อมูลเหล่านี้ภายหลังสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูล

ในกรณีที่พนักงานมีข้อสงสัยเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้พนักงานติดต่อสอบถามผู้ว่าจ้างผ่านทางฝ่ายทรัพยากรบุคคล

นอกเหนือจากการแจ้งรายละเอียดในรูปแบบข้างต้น ผู้ประกอบการอาจมีการแจ้งรายละเอียดในกิจกรรมหรือตำแหน่งเฉพาะ ตัวอย่างเช่น การแจ้งเตือนเรื่องกล้อง CCTV นั้นอาจจะทำเป็นป้ายสัญลักษณ์ โดยมีรายละเอียดเกี่ยวกับการแจ้งดังตัวอย่างข้างล่างนี้

ตัวอย่าง
การเตือนเรื่องกล้องวงจรปิด และการประกาศคุ้มครองข้อมูลส่วนบุคคล ในการใช้กล้องวงจรปิด
(เพื่อนำไปปรับใช้ตามความเหมาะสม)

1. การเตือน บริเวณนี้มีการบันทึกภาพด้วยกล้องวงจรปิด ไม่จำเป็นต้องติดทุกจุดที่มีกล้อง หากสภาพไม่สามารถทำได้ แนะนำให้มีการเตือน ทุกทางเข้าสู่บริเวณ

ตัวอย่างการแจ้งเตือนด้วยป้ายสัญลักษณ์

บริเวณนี้มีการบันทึกภาพด้วยกล้องวงจรปิด

2. ประกาศคุ้มครองข้อมูลส่วนบุคคลในการใช้กล้องวงจรปิดไม่จำเป็นต้องติดทุกจุดที่มีกล้อง หรือทุกจุดที่มีการเตือนตามป้ายโดยอาจจะใช้ QR หรือประกาศฯ ฉบับเต็มติดไว้บางที่ และเก็บไว้พร้อมให้ตรวจสอบ

QR ประกาศคุ้มครองข้อมูลส่วนบุคคลในการใช้กล้องวงจรปิด โปรดดูตาม QR ที่แสดงไว้นี้

ตัวอย่าง
การแจ้งเตือนด้วยการใช้ QR ลิงก์ไปยังประกาศฯ

ตัวอย่างประกาศคุ้มครองข้อมูลส่วนบุคคลในการใช้กล้องวงจรปิด

วัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล

- บริษัทบันทึกและจัดเก็บข้อมูลภาพจากกล้องวงจรปิด (CCTV) ซึ่งติดตั้งอยู่บริเวณอาคารและสถานที่ เพื่อวัตถุประสงค์ในการป้องกันเหตุอันตราย และการกระทำผิดกฎหมายอันอาจเกิดขึ้นในบริเวณที่ทำการของบริษัทฯ รวมทั้งการปฏิบัติตามกฎหมายที่เกี่ยวข้อง ซึ่งบริษัทอาจมีการใช้ และ เผยแพร่ข้อมูลให้กับบุคคลหรือหน่วยงานที่มีอำนาจตามกฎหมายในการใช้ข้อมูลดังกล่าว

ฐานทางกฎหมายที่เกี่ยวข้อง

- ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัทหรือบุคคลอื่น โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของท่าน
- ความจำเป็นในการปฏิบัติตามกฎหมายที่เกี่ยวข้อง

ข้อมูลที่เก็บและระยะเวลาการเก็บ

- เก็บรวมรวมข้อมูลภาพ จากกล้องวงจรปิด และทำการเก็บ ใช้ และเผยแพร่ ตามวัตถุประสงค์ไม่เกิน 90 วัน

สิทธิของเจ้าของข้อมูล :
ท่านสามารถใช้สิทธิตามกฎหมายได้ตามช่องทางต่อไปนี้

- ชื่อผู้ติดต่อ
- ชื่อองค์กร
- ที่อยู่องค์กร
- โทรศัพท์ : 0-2009-xxxx
- อีเมล : online@xxxx.co.th

1.2 การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

สำหรับหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมนั้น มีประกาศเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล[1] ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งข้อกำหนดตามประกาศดังกล่าวถือเป็นมาตรฐานขั้นต่ำที่ให้ไว้เป็นแนวทางสำหรับผู้ประกอบการนำไปปฏิบัติกับ ได้แก่ การเสริมสร้างความตระหนักรู้เกี่ยวกับความสำคัญของข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลที่สำคัญ (access control) โดยอาจจะต้องมีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และมีมาตรการสำหรับอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม เพื่อให้สอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้อาจจะมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เป็นต้น โดยรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยนี้จะอธิบายไว้ในส่วนถัดๆ ไป

1.3 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

กรณีของการเกิดเหตุละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไว้ภายในองค์กรรั่วไหล ผู้ประกอบการซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงานฯ) ทราบโดยไม่ชักช้า[2] อย่างไรก็ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้กำหนดระดับของความเสี่ยงไว้ 3 ระดับ คือ “ไม่มีความเสี่ยง” กรณีนี้อาจจะไม่ต้องแจ้งต่อสำนักงานฯ แต่ผู้ประกอบการอาจจะต้องทำการบันทึกรายละเอียดของการเกิดเหตุไว้ กรณีที่ประเมินแล้ว “มีความเสี่ยงน้อย” ผู้ประกอบการจะต้องแจ้งให้สำนักงานฯ ทราบถึงเหตุของการละเมิดนั้นโดยไม่ชักช้าภายใน 72 ชั่วโมง และกรณีที่ “มีความเสี่ยงสูง” ซึ่งกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ประกอบการจะต้องแจ้งให้สำนักงานฯ ทราบถึงเหตุของการละเมิดนั้นโดยไม่ชักช้าภายใน 72 ชั่วโมง รวมถึงแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมแนวทางการป้องกันความเสียหายที่จะเกิดขึ้นด้วย

กฎหมายกำหนดหลักการสำคัญในการแจ้งเหตุละเมิดว่า ควรเป็นการใช้ภาษาที่ชัดเจนและมีการอธิบายถึงรายละเอียดการละเมิดข้อมูลส่วนบุคคลที่เข้าใจง่าย ในกรณีที่ต้องแจ้งให้กับสำนักงานฯและเจ้าของข้อมูลส่วนบุคคลทราบ จะต้องมีการบรรยายลักษณะของการเหตุละเมิดข้อมูลส่วนบุคคล เช่น ประเภทของข้อมูลที่รั่วไหล จำนวนข้อมูลที่รั่วไหล แจ้งผลกระทบที่จะเกิดขึ้นและอาจเกิดขึ้นในอนาคต รวมถึงมาตรการหรือแนวทางที่จะบรรเทาผลกระทบที่อาจเกิดขึ้น เป็นต้น

---

[1] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

[2] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

1.4 การจัดทำบันทึกรายการ

ในส่วนของการจัดทำบันทึกรายการ (Record of Processing Activity: RoPA) กฎหมายกำหนดไว้ว่าผู้ประกอบการซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลอาจต้องมีการจัดทำบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้[3] ซึ่งวิธีการจัดทำบันทึกนั้นจะเป็นเอกสารกระดาษหรือใช้ระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องมีรายละเอียดดังต่อไปนี้

- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 27 วรรคสาม
- การปฏิเสธคำขอหรือการคัดค้านมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 วรรคหนึ่ง (1)

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39

กฎหมายไม่ได้กำหนดรูปแบบของบันทึกรายการไว้ตายตัว เป็นเพียงการกำหนดสาระสำคัญของรายการที่ต้องบันทึกไว้เท่านั้น นอกจากนี้ ผู้ประกอบการซึ่งอยู่ในขอบเขตของการเป็นกิจการขนาดเล็กจะได้รับการยกเว้นตามกฎหมาย ทำให้ไม่ต้องจัดทำบันทึกรายการดังกล่าว ซึ่งจะได้อธิบายรายละเอียดในหัวข้อถัดไป

2. ข้อยกเว้นของผู้ประกอบการซึ่งเป็นกิจการขนาดเล็ก

เนื่องจากสภาพของสังคมในปัจจุบันและลักษณะในการประกอบธุรกิจที่มีหลากหลายขนาดแตกต่างกันไป จึงทำให้ความสามารถในการปฏิบัติหน้าที่ตามกฎหมายย่อมแตกต่างกันไปด้วย ดังนั้น กฎหมายจึงได้กำหนดหลักเกณฑ์และข้อยกเว้นให้สำหรับผู้ประกอบการที่ประกอบธุรกิจโดยมีลักษณะเป็นกิจการขนาดเล็กตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565 เพื่อให้สอดคล้องกับสภาพของสังคมและการประกอบกิจการ

2.1 ผู้ประกอบการซึ่งเป็นกิจการขนาดกลางและขนาดย่อม

นอกจากการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการประมวลผลข้อมูลส่วนบุคคล และการจัดให้มีมาตรฐานการรักษาความปลอดภัยตามที่กฎหมายกำหนดแล้ว รวมถึงผู้ประกอบการยังมีหน้าที่ต้องจัดทำบันทึกรายการตามรายละเอียดในข้อ 1.4 ด้วย เพื่อให้สามารถตรวจสอบและทราบได้ถึงกระบวนการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมต่างๆ ได้อย่างชัดเจน อย่างไรก็ตาม ผู้ประกอบการบางประเภทได้รับการยกเว้นไม่ต้องจัดทำบันทึกรายการ โดยประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565 กำหนดประเภทของกิจการที่ได้รับการยกเว้นไว้ดังต่อไปนี้

ผู้ประกอบการที่ถือว่าอยู่ในขอบเขตของกิจการขนาดเล็กจะต้องมีลักษณะอย่างใดอย่างหนึ่งที่กำหนดไว้ในประกาศฯ โดยการกำหนดลักษณะดังกล่าวมีความสอดคล้องกับการประกอบกิจการของวิสาหกิจที่มีขนาดย่อมและขนาดกลาง ดังต่อไปนี้

ตารางลักษณะของการเป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมาย

ลักษณะของกิจการ	กิจการ	การจ้างงานต่อปี	รายได้ต่อปี
วิสาหกิจรายย่อย	กิจการที่ผลิตสินค้า	ไม่เกิน 5 คน	ไม่เกิน 1.8 ล้านบาท
	กิจการที่ให้บริการ ค้าส่ง ค้าปลีก		
วิสาหกิจขนาดย่อม (Small)	กิจการที่ผลิตสินค้า	ไม่เกิน 50 คน	ไม่เกิน 100 ล้านบาท
	กิจการที่ให้บริการ ค้าส่ง ค้าปลีก	ไม่เกิน 30 คน	ไม่เกิน 50 ล้านบาท
วิสาหกิจขนาดกลาง (Medium)	กิจการที่ผลิตสินค้า	เกินกว่า 50 คน แต่ไม่เกิน 200 คน	เกินกว่า 100 ล้านแต่ไม่เกิน 500 ล้านบาท
	กิจการที่ให้บริการ ค้าส่ง ค้าปลีก	เกินกว่า 30 คน แต่ไม่เกิน 100 คน	เกินกว่า 50 ล้านแต่ไม่เกิน 300 ล้านบาท

ที่มา: กฎกระทรวงกำหนดลักษณะของวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2562

นอกจากนี้ ประกาศฯ ยังกำหนดให้วิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชน[4] วิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคม[5] และองค์กรอื่น เช่น สหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์ มูลนิธิ สมาคม องค์กรศาสนา องค์กรที่ไม่แสวงหากำไร หรือการทำกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน ให้อยู่ในขอบเขตของการเป็นกิจการขนาดเล็กอีกด้วย กล่าวคือ หากเป็นองค์กรที่ระบุอยู่ในประกาศฯ อย่างใดอย่างหนึ่งแล้วย่อมได้รับการยกเว้นไม่ต้องจัดทำบันทึกรายการตามกฎหมาย แต่ยังคงมีหน้าที่อื่นตามกฎหมายที่คงต้องปฏิบัติตามอยู่ เช่น การแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ หรือการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ตามที่ได้อธิบายไปแล้วในข้างต้น

อย่างไรก็ดี แม้ว่าผู้ประกอบการจะอยู่ภายใต้ขอบเขตของการประกอบกิจการขนาดเล็กแต่หากปรากฏว่ามีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือเป็นข้อมูลส่วนบุคคลอ่อนไหวตามที่ระบุไว้ในมาตรา 26 ในกรณีดังกล่าวนี้ก็ไม่ได้อยู่ภายใต้ข้อยกเว้นในการจัดทำบันทึกรายการ

2.2 ผู้ประกอบการซึ่งเป็นกิจการขนาดเล็กและเป็นผู้ให้บริการตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จากหลักเกณฑ์ที่กำหนดไว้ในประกาศฯ มีส่วนที่ต้องพิจารณาต่อว่า นอกจากจะต้องเป็นผู้ประกอบการที่มีกิจการขนาดเล็กตามเงื่อนไขข้างต้นแล้ว จะต้องไม่เป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กล่าวคือ แม้ว่าเป็นผู้ประกอบการที่เป็นวิสาหกิจขนาดย่อมหรือขนาดกลางและมีเกณฑ์การจ้างงานและรายได้ต่อปีเป็นไปตามเกณฑ์ที่กำหนดไว้ แต่หากปรากฏว่า ผู้ประกอบการดังกล่าวประกอบกิจการที่ถือได้ว่าเป็น “ผู้ให้บริการ”[6] ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider) ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชันต่างๆ (Content and

---

[4] พระราชบัญญัติส่งเสริมวิสาหกิจชุมชน พ.ศ. 2548 มาตรา 3
“วิสาหกิจชุมชน” หมายความว่า กิจการของชุมชนเกี่ยวกับการผลิตสินค้า การให้บริการ หรือการอื่นๆ ที่ดำเนินการโดยคณะบุคคลที่มีความผูกพัน มีวิถีชีวิตร่วมกันและรวมตัวกันประกอบกิจการดังกล่าว ไม่ว่าจะเป็นนิติบุคคลในรูปแบบใดหรือไม่เป็นนิติบุคคล เพื่อสร้างรายได้และเพื่อการพึ่งพาตนเองของครอบครัว ชุมชนและระหว่างชุมชน ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

[5] พระราชบัญญัติส่งเสริมวิสาหกิจเพื่อสังคม พ.ศ. 2562 มาตรา 3
“วิสาหกิจเพื่อสังคม” หมายความว่า บริษัท ห้างหุ้นส่วนนิติบุคคล หรือนิติบุคคลอื่น ที่ตั้งขึ้นตามกฎหมายไทย ซึ่งดำเนินกิจการเกี่ยวกับการผลิต การจำหน่ายสินค้า หรือการบริการ โดยมีวัตถุประสงค์เพื่อสังคมเป็นเป้าหมายหลักของกิจการ และได้รับการจดทะเบียนตามพระราชบัญญัตินี้

[6] ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ข้อ 4
“ผู้ให้บริการ” หมายความว่า (1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนาม หรือเพื่อประโยชน์ของบุคคลอื่น (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

Application Service Provider) และผู้ให้บริการดิจิทัล (Digital Service Provider) ที่ใช้เครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นส่วนหนึ่งของการให้บริการ เป็นต้น ผู้ประกอบการดังกล่าวนั้นจะไม่ได้รับการยกเว้นตามประกาศฯ กล่าวคือ ผู้ประกอบการที่เป็นผู้ให้บริการตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ยังคงต้องปฏิบัติตามกฎหมายในการจัดทำบันทึกรายการตามรายละเอียดที่กำหนดไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ดี กฎหมายเล็งเห็นว่า การเป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์นั้นมีหลายประเภท ซึ่งมีอยู่ประเภทหนึ่งที่มีลักษณะการประกอบกิจการและศักยภาพเป็นไปตามกิจการขนาดเล็ก คือ ผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ต ซึ่งหากผู้ประกอบการเข้าเงื่อนไขของการเป็นผู้ให้บริการประเภทดังกล่าว เช่น ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café) ผู้ให้บริการร้านเกมออนไลน์ (Game Online) หรือผู้ให้บริการประเภทเกมส์หรือสันทนาการประเภท Virtual Reality หรือ e-Sport เป็นต้น จะได้รับการยกเว้นตามประกาศฯ คือไม่ต้องจัดทำบันทึกรายการดังกล่าว

ดังนั้น จึงสามารถสรุปได้ว่า ผู้ประกอบการซึ่งเป็นกิจการขนาดเล็กที่จะได้รับการยกเว้นในการจัดทำบันทึกรายการจะต้องเป็นผู้ประกอบการที่ประกาศฯกำหนดและจะต้องไม่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือเป็นข้อมูลส่วนบุคคลอ่อนไหวตามที่ระบุไว้ในมาตรา 26 และหากเป็นผู้ประกอบการที่เป็นผู้ให้บริการตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จะต้องปรากฏว่าเป็นผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ตเท่านั้นจึงจะอยู่ภายใต้ข้อยกเว้นตามประกาศฯ ดังกล่าว

บทที่ 3 การจัดทำบันทึกรายการ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ให้ผู้ประกอบการซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกรายการ และในกรณีที่ผู้ประกอบการมีบทบาทเป็นผู้ประมวลผลข้อมูลส่วนบุคคลด้วยจะต้องจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลด้วยเช่นกัน โดยในส่วนนี้คู่มือจะอธิบายเกี่ยวกับการจัดทำบันทึกรายการทั้ง 2 แบบ

1. วัตถุประสงค์ของการจัดทำบันทึกรายการและบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์ของการจัดทำบันทึกรายการมีเพื่อรวบรวมข้อมูลเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายใต้การดำเนินการของผู้ประกอบการ (ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล) ซึ่ง**โดยทั่วไปแล้วผู้ควบคุมข้อมูลส่วนบุคคลทุกคนมีหน้าที่จะต้องจัดทำบันทึกรายการ เว้นแต่จะเป็นกิจการขนาดกลางและขนาดย่อม** ซึ่งรายละเอียดของข้อยกเว้นดังได้กล่าวในบทที่ 2 นอกจากนี้ เมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลหรือมีเหตุจำเป็น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้สำนักงานฯ สามารถตรวจสอบบันทึกรายการได้

อย่างไรก็ดี สิ่งสำคัญที่ต้องทำความเข้าใจก็คือ การจัดทำบันทึกรายการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นไม่ใช่การเก็บ log ในลักษณะเดียวกันกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่กำหนดให้ผู้ให้บริการอินเทอร์เน็ตจะต้องเก็บบันทึกข้อมูลการใช้งานอินเทอร์เน็ต สิ่งที่ต้องให้ความสำคัญคือรูปแบบการทำบันทึกดังกล่าวจะต้องแก้ไข เปลี่ยนแปลง และเข้าถึงได้ง่าย ดังนั้น การทำบันทึกในรูปแบบไฟล์อิเล็กทรอนิกส์ผ่านโปรแกรมพื้นฐานแบบสเปรดชีต (spreadsheet) เช่น MS Excel เป็นต้น

2. การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ควบคุมข้อมูลส่วนบุคคลกฎหมายกำหนดรายละเอียดของบันทึกรายการของกิจกรรมกาประมวลผลข้อมูลส่วนบุคคลเอาไว้ ดังนี้[7]

- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ชื่อ และรายละเอียดการติดต่อขององค์กร รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ได้แก่ คำอธิบายเกี่ยวกับหมวดหมู่ของเจ้าของข้อมูลส่วนบุคคล (categories of individual) หรือหมวดหมู่ข้อมูลส่วนบุคคล (categories of personal data) ที่องค์กรทำการประมวลผล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม กล่าวคือ หากองค์กรใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 องค์กรต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39 ด้วย ซึ่งในทางปฏิบัติหมายความถึง (1) ให้ระบุฐานทางกฎหมายในการประมวลผล และ (2) ให้ระบุการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก
- การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 วรรคสาม (สิทธิในการเข้าถึง) มาตรา 31 วรรคสาม (สิทธิในการขอให้โอนข้อมูล) มาตรา 32 วรรคสาม (สิทธิในการคัดค้านการประมวลผล) และมาตรา 36 วรรคหนึ่ง (สิทธิในการขอแก้ไขข้อมูลให้ถูกต้อง) ตามเงื่อนไขที่กฎหมายกำหนด
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

ในส่วนของรูปแบบการบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลนั้น กฎหมายไม่ได้มีรูปแบบตายตัว เพียงแต่ต้องจัดทำเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ สิ่งสำคัญที่ต้องทำความเข้าใจก็คือ รูปแบบการทำบันทึกดังกล่าวจะต้องแก้ไข เปลี่ยนแปลง และเข้าถึงได้ง่าย ดังนั้น การทำบันทึกในรูปแบบไฟล์อิเล็กทรอนิกส์ผ่านโปรแกรมพื้นฐานแบบสเปรดชีต (spreadsheet) เช่น MS Excel เป็นต้น

สำหรับแนวทางในการกรอกข้อมูลลงในบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณารายละเอียดที่ปรากฏอยู่ในประกาศการคุ้มครองข้อมูลส่วนบุคคล (privacy notice)

ตัวอย่าง บันทึกรายการ (Record of Processing Activities: ROPA) สำหรับผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 1: ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล	
ผู้ควบคุมข้อมูลส่วนบุคคล	
ชื่อ-สกุล/ชื่อองค์กร	บริษัท เจ้าป่าเดอะแคท จำกัด
ที่อยู่	565 ซอยรามคำแหง 39 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ 10310
อีเมล	jaopaa@thecat.com
เบอร์โทรศัพท์	XX-XXX-XXX
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (ถ้ามี)	
ชื่อ-สกุล	คุณต้นสน รักไดโนเสาร์
ที่อยู่	566 ซอยรามคำแหง 40 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ 10311
อีเมล	cooper@thedog.com
เบอร์โทรศัพท์	XX-XXX-XXX

ส่วนที่ 2: บันทึกรายการ					
รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล (เก็บรวบรวม ใช้ เปิดเผย)					**มาตรการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1)**
ชื่อกิจกรรม	วัตถุประสงค์	ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	การใช้ / เปิดเผย	ระยะเวลา	มาตรการรักษาความปลอดภัย
คำอธิบาย: ชื่อกิจกรรมอาจตั้งขึ้นจากรูปแบบการประกอบธุรกิจหรือลักษณะของกิจกรรมที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	คำอธิบาย: การกำหนดวัตถุประสงค์หลักของกิจกรรมจะต้องพิจารณาว่ามีการทำกิจกรรมการประมวลผลเพราะอะไร ซึ่งโดยทั่วไปแล้วกิจกรรมหนึ่งจะมีวัตถุประสงค์หลักเพียงวัตถุประสงค์เดียว	คำอธิบาย: ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ควรระบุ - หมวดหมู่ของข้อมูลส่วนบุคคล - กลุ่มของบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล	คำอธิบาย: อธิบายลักษณะการใช้ข้อมูลส่วนบุคคลดังกล่าว หรือการเปิดเผยข้อมูลส่วนบุคคล โดยการอ้างอิงว่าในแต่ละกิจกรรมมีการอาศัยฐานการปฏิบัติตามกฎหมายในมาตรา 24 หรือมาตรา 26	คำอธิบาย: การระบุระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลนั้นเพื่อให้ทราบว่าข้อมูลส่วนบุคคลจะถูกจัดเก็บไว้เป็นระยะเวลานานเพียงใด	คำอธิบาย: ระบุมาตรการรักษาความปลอดภัย
ตัวอย่าง: การจัดเก็บประวัติผู้สมัครงาน	ตัวอย่าง: เพื่อใช้ในการพิจารณาคุณสมบัติผู้สมัครงาน	ตัวอย่าง: ข้อมูลระบุตัวตน และข้อมูลการติดต่อของผู้สมัครเป็นพนักงาน	ตัวอย่าง: ใช้ในการพิจารณาคุณสมบัติผู้สมัครงาน ตามฐานสัญญา (มาตรา 24 (3))	ตัวอย่าง: 3 ปี หลังจากการยื่นใบสมัคร	ตัวอย่าง: การกำหนดสิทธิเข้าถึง (access control) เฉพาะเจ้าหน้าที่ฝ่ายบุคคลและผู้บริหาร
ตัวอย่าง: การจัดเก็บฐานข้อมูลลูกค้า	ตัวอย่าง: เพื่อใช้ในการให้บริการกับลูกค้า	ตัวอย่าง: ข้อมูลระบุตัวตน เบอร์โทร ที่อยู่ ข้อมูลการให้บริการแก่ลูกค้า	ตัวอย่าง: ใช้ในการให้บริการตามฐานสัญญา (มาตรา 24 (3))	ตัวอย่าง: 10 ปี	ตัวอย่าง: การกำหนดสิทธิเข้าถึง (access control) / การจัดเก็บแบบเข้ารหัส (encrypted storage)
การใช้สิทธิ				**หมายเหตุ**	
สิทธิของเจ้าของข้อมูลส่วนบุคคล		การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล			
คำอธิบาย: การระบุสิทธิของเจ้าของข้อมูลส่วนบุคคลในกรณีจะเป็นไปตามหมวด 3 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล		คำอธิบาย: การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลอาจจะระบุโดยการทำลิงก์เชื่อมโยงใน Excel ไป sheet อื่นที่ลงรายละเอียดการปฏิเสธสิทธิในกิจกรรมนั้นแต่ละครั้ง		
ตัวอย่าง: สิทธิขอแก้ไขข้อมูล ฯลฯ		ตัวอย่าง: sheet 2			

หมายเหตุ ในการจัดทำตารางบันทึกรายการ ผู้ประกอบการควรจะจัดทำตารางเป็นแนวนอนเชื่อมต่อกันไประหว่าง 1) รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล 2) มาตรการรักษาความมั่นคงปลอดภัย 3) การใช้สิทธิ และ 4) หมายเหตุ

3. การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีผู้ประมวลผลข้อมูลส่วนบุคคล กฎหมายกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องควบคุมและป้องกันไม่ให้ผู้ประมวลผลข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ และให้ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

รายละเอียดของบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคลถูกกำหนดไว้ในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565[8] ข้อ 3 ดังนี้

- ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลและตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน
- ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน
- ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมถึงสถานที่ติดต่อและวิธีการติดต่อในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
- ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 40 วรรคหนึ่ง (2)

อย่างไรก็ดี เมื่อเปรียบเทียบรายการข้อมูลที่ต้องบันทึกในบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 39 และกฎเกณฑ์ที่ประกาศฯกำหนด เนื่องจากผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่แตกต่างจากผู้ควบคุมข้อมูลส่วนบุคคลและจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลในลักษณะและด้วยวัตถุประสงค์ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล จึงทำให้มีข้อมูลที่ต้องบันทึกในบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่แตกต่างจากรายการที่กำหนดในมาตรา 39 โดยรายการข้อมูลส่วนใหญ่ที่ประกาศฉบับนี้ กำหนดให้บันทึก

[8] ประกาศฉบับนี้มีผลใช้บังคับเมื่อพ้นระยะเวลา 180 วัน นับตั้งแต่ประกาศในราชกิจจานุเบกษา

เป็นข้อมูลที่มักทำการตกลงไว้ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลอยู่แล้ว การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลจึงสามารถช่วยสร้างความชัดเจนเกี่ยวกับขอบเขตของหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล และลดความเสี่ยงในการทำกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกเหนือขอบเขตที่ตกลงไว้กับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่ภาระในการปฏิบัติตามกฎหมายที่สูงมากขึ้น

ในส่วนของรูปแบบการบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคลนั้น กฎหมายไม่ได้มีรูปแบบตายตัว เพียงแต่ต้องจัดทำเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ สิ่งสำคัญที่ต้องทำความเข้าใจ คือ รูปแบบการทำบันทึกดังกล่าวจะต้องแก้ไข เปลี่ยนแปลง และเข้าถึงได้ง่าย ดังนั้น การทำบันทึกในรูปแบบไฟล์อิเล็กทรอนิกส์ผ่านโปรแกรมพื้นฐานแบบสเปรดชีต (spreadsheet) เช่น MS Excel เป็นต้น

ตัวอย่าง บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ส่วนที่ 1: ข้อมูลติดต่อบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล [ข้อ 3 (1) – (3)]	
ผู้ประมวลผลข้อมูลส่วนบุคคล (และตัวแทน หากมี)	
ชื่อ-สกุล/ชื่อองค์กร	บริษัท เจ้าป่าเดอะแคท จำกัด
ที่อยู่	565 ซอยรามคำแหง 39 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ 10310
อีเมล	jaopaa@thecat.com
เบอร์โทรศัพท์	XX-XXX-XXX
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (หากมี)	คุณต้นสน รักไดโนเสาร์ + ข้อมูลติดต่อ

<table>
<tr><td colspan="4">ส่วนที่ 2: บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล</td></tr>
<tr><td>ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล</td><td colspan="3">รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล [ข้อ 3 (4)]</td></tr>
<tr><td>ผู้ควบคุมข้อมูลส่วนบุคคล (และตัวแทน หากมี)</td><td>ประเภทหรือลักษณะ (ชื่อกิจกรรม)</td><td>ข้อมูลส่วนบุคคล</td><td>วัตถุประสงค์</td></tr>
<tr><td rowspan="2">ชื่อ-สกุล/ชื่อองค์กร บริษัท คูเป้อร์เดอะด็อก จำกัด
ที่อยู่ 566 ซอยรามคำแหง 40 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ 10311
อีเมล cooper@thedog.com
เบอร์โทรศัพท์ XX-XXX-XXX
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (หากมี) คุณดินดาวเดือน + ข้อมูลติดต่อ</td><td><u>คำอธิบาย</u>: ชื่อกิจกรรมนั้นอาจตั้งขึ้นโดยพิจารณารูปแบบการประกอบธุรกิจหรือลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของตน</td><td><u>คำอธิบาย</u>: การระบุหมวดหมู่ของข้อมูลส่วนบุคคลเพื่อกำหนดว่าภายใต้กิจกรรมการประมวลผลข้อมูลส่วนบุคคลนี้ประกอบไปด้วยข้อมูลส่วนบุคคลในลักษณะใด</td><td><u>คำอธิบาย</u>: การกำหนดวัตถุประสงค์หลักของกิจกรรม จะต้องพิจารณาว่ามีการทำกิจกรรมการประมวลผลเพราะอะไร ซึ่งโดยทั่วไปแล้วกิจกรรมหนึ่งจะมีวัตถุประสงค์หลักเพียงวัตถุประสงค์เดียว</td></tr>
<tr><td><u>ตัวอย่าง</u>: การวิเคราะห์พฤติกรรมการใช้งานเว็บไซต์ของลูกค้า</td><td><u>ตัวอย่าง</u>: ข้อมูลระบุตัวตน/ข้อมูลการติดต่อ/ข้อมูลทางการเงิน/ข้อมูลส่วนบุคคลละเอียดอ่อน</td><td><u>ตัวอย่าง:</u> เพื่อใช้ในการทำการตลาดและแนะนำสินค้า</td></tr>
<tr><td colspan="2">การโอนข้อมูลไปยังต่างประเทศ (หากมี) [ข้อ 3 (5)]</td><td colspan="2">มาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 40 วรรคหนึ่ง (2) [ข้อ 3 (6)]</td></tr>
<tr><td>ชื่อประเทศและองค์กร/บุคคลปลายทาง</td><td>คำอธิบายมาตรการรักษาความปลอดภัย</td><td colspan="2">บันทึกการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล (หากมี)</td></tr>
<tr><td><u>คำอธิบาย</u>: การระบุชื่อประเทศที่มีการโอนข้อมูลส่วนบุคคลไปถึงนั้นเพื่อให้ทราบว่าประเทศปลายทางดังกล่าวนั้นอยู่ภายใต้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพียงพอหรือไม่</td><td><u>คำอธิบาย</u>: การระบุคำอธิบายทั่วไปของมาตรการรักษาความปลอดภัยทางเทคนิคและองค์กรนั้นสามารถกำหนดประเภทของมาตรการก็ได้</td><td colspan="2"><u>คำอธิบาย</u>: นอกเหนือจากการกำหนดมาตรการการรักษาความปลอดภัยของข้อมูลแล้ว มาตรา 40 วรรคหนึ่ง (2) ยังกำหนดหน้าที่ในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลภายใต้การดูแลของผู้ประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมด้วย</td></tr>
<tr><td><u>ตัวอย่าง</u>: สหรัฐอเมริกา, บริษัท ไฉไล จำกัด</td><td><u>ตัวอย่าง</u>: การกำหนดสิทธิเข้าถึง (access control) / การจัดเก็บแบบเข้ารหัส (encrypted storage)</td><td colspan="2">กรณีไม่มีให้ใส่ N/A</td></tr>
</table>

หมายเหตุ ในการจัดทำตารางบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ผู้ประกอบการควรจะจัดทำตารางเป็นแนวนอนเชื่อมต่อกันไประหว่าง 1) รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล 2) มาตรการรักษาความมั่นคงปลอดภัย 3) การใช้สิทธิ และ 4) หมายเหตุ

บทที่ 4 การจัดการมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหน้าที่พื้นฐานอีกประการหนึ่งที่ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการ

1. วัตถุประสงค์และความจำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ[9] โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

วัตถุประสงค์ของการรักษาความปลอดภัยมีวัตถุประสงค์เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และอำนาจในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งกฎหมายรับรองไว้ให้ ด้วยเหตุนี้ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหน้าที่ประการหนึ่งตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล (รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคล) จะต้องปฏิบัติเพื่อป้องกันมิให้เกิดสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งจะทำให้เกิดภัยคุกคามต่อความปลอดภัยของข้อมูลส่วนบุคคลหรือตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเรียกว่า “การละเมิดข้อมูลส่วนบุคคล”

2. แนวทางการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล

ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ผู้ควบคุมมีหน้าที่จะต้องดำเนินการ 2 ประการ คือ การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น และการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

2.1 การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น

ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องพิจารณาปัจจัยในการประเมินความเสี่ยง 3 ด้านประกอบกัน คือ ลักษณะของข้อมูล จำนวนของข้อมูลในการควบคุม และผลกระทบที่อาจจะเกิดขึ้นจากข้อมูล โดยเฉพาะอย่างยิ่งผู้ประกอบธุรกิจขนาดกลางและขนาดย่อม (SMEs) นั้นควรเลือกใช้มาตรการที่เหมาะสมกับขนาดและความจำเป็นของตนเอง

[9] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3

- **ประเภทของข้อมูลส่วนบุคคล** การพิจารณาปัจจัยประเภทนี้ หากข้อมูลส่วนบุคคลใดเป็นข้อมูลส่วนบุคคลทั่วไป ที่ในการใช้ข้อมูลส่วนบุคคลไม่ก่อให้เกิดความเสียหายกับเจ้าของข้อมูลส่วนบุคคลมาก มาตรการที่นำมาใช้อาจจะไม่ต้องเข้มงวดมาก เช่น การเก็บบันทึกหรือเอกสารที่ระบุข้อมูลส่วนบุคคลให้ปลอดภัย โดยอาจจะเก็บไว้ในตู้เอกสารให้เรียบร้อย เป็นต้น แต่หากเป็นข้อมูลส่วนบุคคลที่มีความเสี่ยงเพิ่มมากขึ้น โดยเป็นข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 วรรคหนึ่ง เช่น การเก็บบันทึกหรือเอกสารที่เกี่ยวกับประวัติอาชญากรรมของผู้สมัคร ซึ่งเคยเป็นผู้ต้องโทษและได้พ้นโทษมาแล้ว หากข้อมูลดังกล่าวหลุดรั่วออกไปอาจจะทำให้เกิดการเลือกปฏิบัติต่อเจ้าของข้อมูลส่วนบุคคลได้ เป็นต้น ฉะนั้น ในกรณีของการจัดเก็บข้อมูลประเภทนี้อาจจะต้องมีการแยกเก็บข้อมูลดังกล่าวไว้จากข้อมูลส่วนอื่น และกำหนดสิทธิให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้นที่จะเข้าถึงข้อมูลดังกล่าว เช่น การเก็บข้อมูลประวัติอาชญากรรมไว้ในตู้เอกสารเฉพาะ และให้เฉพาะเจ้าหน้าที่ฝ่ายบุคคลเท่านั้นที่มีกุญแจ เป็นต้น

> ข้อมูลส่วนบุคคลอ่อนไหว ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ และข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

- **จำนวนของข้อมูลในการควบคุม** การพิจารณาปัจจัยประเภทนี้จะต้องคำนึงถึงจำนวนของข้อมูลส่วนบุคคลภายใต้กิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นๆ ประกอบ กรณีของสถานประกอบกิจการที่มีรายชื่อลูกค้าจำนวนน 100 ราย กับจำนวน 10,000 ราย ย่อมจะมีความแตกต่างกัน ซึ่งมาตรการที่จะนำมาใช้ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลย่อมจะมีความแตกต่างกัน ในกรณีที่มีบุคคลเข้ามามีส่วนเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก องค์กรควรพิจารณากำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล ให้มีเฉพาะผู้มีส่วนเกี่ยวข้องเท่านั้น
- **ผลกระทบที่อาจจะเกิดขึ้นจากข้อมูล (impact)** การพิจารณาปัจจัยประเภทนี้ ควรคำนึงถึงผลกระทบที่อาจจะเกิดขึ้นหากข้อมูลส่วนบุคคลนั้นรั่วไหลออกไป เช่น ในกรณีของร้านทำผมซึ่งมีลูกค้าเป็นดาราหรือผู้มีชื่อเสียงมาใช้บริการ ผลกระทบที่เกิดขึ้นจากการรั่วไหลของข้อมูลส่วนบุคคลดังกล่าวอาจจะมีมากกว่าร้านทำผมกรณีปกติ เป็นต้น

2.2 การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

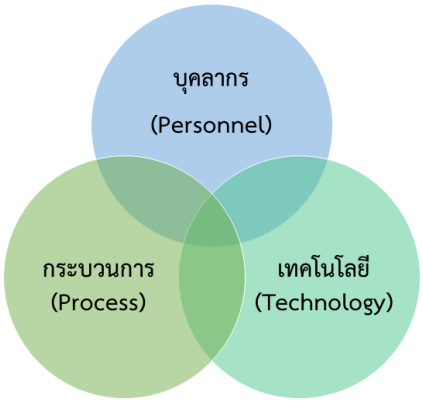
ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการเกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล โดยประกอบด้วยมาตรการอย่างน้อยที่กำหนดไว้ในข้อ 4 (6) โดยพิจารณามาตรการให้เหมาะสมกับลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

- การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (access control) ที่มีการพิสูจน์และยืนยันได้ว่า บุคคลใดเป็นผู้เข้าถึงข้อมูลส่วนบุคคลดังกล่าวได้ และการอนุญาตหรือกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม เช่น กำหนดให้สิทธิการเข้าถึงข้อมูลเกี่ยวกับพนักงานบริษัท เฉพาะพนักงานฝ่ายทรัพยากรบุคคล เป็นต้น
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม โดยกำหนดให้ผู้ใช้งานมีสิทธิเข้าถึงข้อมูลส่วนบุคคล ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน การจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งานและการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. การทบทวนมาตรการรักษาความมั่นคงปลอดภัยในปัจจุบัน

ในการทบทวนมาตรการรักษาความมั่นคงปลอดภัยในปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องพิจารณาทบทวนมาตรการตามปัจจัยดังกล่าวข้างต้นอย่างสม่ำเสมอเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยทันที และในการทบทวนมาตรการรักษาความมั่นคงปลอดภัยควรจะต้องพิจารณาว่า การทบทวนมาตรการทั้งในด้านของบุคลากร กระบวนการ และเทคโนโลยีประกอบกัน

ปัจจัยในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล



ที่มา: ปรับปรุงจาก IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (4 edt, IT Governance Publishing Ltd 2020) 82.

ในส่วนของรายละเอียดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลพิจารณาได้จาก ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ภาคผนวก

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก

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

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ที่ได้รับยกเว้นไม่ต้องดำเนินการตามมาตรา ๓๙ วรรคหนึ่ง (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) จะต้องมีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

(๑) เป็นวิสาหกิจขนาดย่อมหรือวิสาหกิจขนาดกลางตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม

(๒) เป็นวิสาหกิจชุมชนหรือเครือข่ายวิสาหกิจชุมชนตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจชุมชน

(๓) เป็นวิสาหกิจเพื่อสังคมหรือกลุ่มกิจการเพื่อสังคมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจเพื่อสังคม

(๔) เป็นสหกรณ์ ชุมนุมสหกรณ์ หรือกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์

(๕) เป็นมูลนิธิ สมาคม องค์กรศาสนา หรือองค์กรที่ไม่แสวงหากำไร

(๖) เป็นกิจการในครัวเรือนหรือกิจการอื่นในลักษณะเดียวกัน

ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามวรรคหนึ่ง จะต้องไม่เป็นผู้ให้บริการที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เว้นแต่จะเป็นผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ต ให้ได้รับยกเว้นตามวรรคหนึ่ง

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กที่ได้รับยกเว้นตามวรรคหนึ่ง ไม่รวมถึงกรณีที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่

กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

ข้อ ๔ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕

เธียรชัย ณ นคร

ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ
ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๔๐ วรรคหนึ่ง (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๒) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๓) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๔) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(๕) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(๖) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๔๐ วรรคหนึ่ง (๒)

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือ

ในรูปแบบอิเล็กทรอนิกส์ก็ได้ ทั้งนี้ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าวจะต้องเข้าถึงได้ง่าย และสามารถแสดงให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายตรวจสอบได้อย่างรวดเร็วเมื่อมีการร้องขอ

ข้อ ๔ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

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

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

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

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

(information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

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

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

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

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

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning) การบริหารจัดการสิทธิการเข้าถึง

ตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

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

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

(๗) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ ๔ เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๖ ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำตามข้อ ๔ โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อ ๗ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

ข้อ ๘ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

คู่มือ PDPA
สำหรับผู้ประกอบการ SMEs

คณะผู้จัดทำ

นายเวทางค์ พ่วงทรัพย์	รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายปฐมพงษ์ ขาวจันทร์	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายณรงค์เดช วัชระภาสร	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นางสาวธีรวดี สุภาวนิตย์	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายขวัญชัย คงสุข	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายทวีสิทธิ์ เพ็ญรัศมีพูนสุข	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นางสุนทรีย์ ส่งเสริม	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายเขมภัทร ทฤษฎิคุณ	สถาบันวิจัยเพื่อการพัฒนาประเทศไทย
นางสาวดลดา คะสาร	สถาบันวิจัยเพื่อการพัฒนาประเทศไทย
นางสาววิชญาดา อำพนกิจวิวัฒน์	สถาบันวิจัยเพื่อการพัฒนาประเทศไทย

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ทำหน้าที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติฯ
อาคารรัฐประศาสนภักดี (อาคารบี) ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์: 1111 หรือ 02-142-1033 หรือ 02-141-6993
เฟสบุ๊ค: https://www.facebook.com/pdpc.th
เว็บไซต์: http://www.pdpc.or.th