



คลองจั่น เขตบางกะปิ กทม. ๑๐๒๔๐ โทร ๐-๒๓๕๑-๗๗๗๗

ประกาศการเคหะแห่งชาติ  
เรื่อง นโยบาย หรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล  
และผู้ประมวลผลข้อมูลส่วนบุคคล  
(Outsourcing Policy for Personal Data Processing)

การเคหะแห่งชาติ (“องค์กร”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 ซึ่งกำหนดให้กรณีที่ทำเนิงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล การเคหะแห่งชาติในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีข้อตกลงระหว่างองค์กรจึงได้กำหนด นโยบาย และแนวปฏิบัติในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล (“นโยบาย”) ฉบับนี้ขึ้น เพื่อกำหนดแนวทางและรายละเอียดในการทำข้อตกลงหรือสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ดังปรากฏรายละเอียดในนโยบายฉบับนี้

1. วัตถุประสงค์

นโยบายในการทำข้อตกลง หรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing) ฉบับนี้ มีวัตถุประสงค์ ดังต่อไปนี้

1.1 เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย

1.2 เพื่อกำหนดขั้นตอนหรือมาตรฐานการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคล

1.3 เพื่อกำหนดแนวทางในการปฏิบัติงานซึ่งเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

1.4 เพื่อสร้างความเชื่อมั่นในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลต่อบุคคล ลูกค้า ผู้ใช้บริการ ตลอดจนบุคคลอื่น ๆ ซึ่งมีส่วนได้เสียหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล

2. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ จะถูกนำมาบังคับใช้กับผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการประมวลข้อมูลส่วนบุคคล ภายใต้คำสั่งหรือในนามขององค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

### 3. นิยาม

“สัญญาการประมวลผลข้อมูล” หมายความว่า สัญญาการประมวลผลข้อมูล (Data Processing Agreement) คือ ข้อตกลงหรือสัญญาระหว่าง ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล อาทิ การดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เป็นต้น

“องค์กร” หมายความว่า การเคหะแห่งชาติ

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลละเอียดอ่อน” หมายความว่า ข้อมูลที่เป็นเรื่องส่วนบุคคลโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและอาจเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของข้อมูล (Data Owner) หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลนี้จะหมายถึงบุคคลธรรมดาเท่านั้น และไม่รวมถึง “นิติบุคคล” (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท สมาคม มูลนิธิ หรือองค์กรอื่นใด

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคล หรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคล หรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

### 4. การพิจารณาจัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

องค์กรจะมีการจัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) เมื่อองค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มอบหมายให้บุคคลหรือนิติบุคคลซึ่งมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามขององค์กร

ทั้งนี้ เงื่อนไขในการพิจารณาบุคคล หรือนิติบุคคลที่องค์กรใช้บริการว่าเข้าองค์ประกอบเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเข้าข่ายที่จะต้องจัดให้มีสัญญาการประมวลผลข้อมูลส่วนบุคคลหรือไม่นั้นพิจารณาเบื้องต้น ดังนี้

4.1 คู่สัญญาซึ่งเป็นบุคคลหรือนิติบุคคล เป็นผู้เก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของผู้ควบคุมข้อมูลหรือไม่ หากบุคคลหรือนิติบุคคลดังกล่าว ไม่ได้ดำเนินการเกี่ยวข้องกับข้อมูลส่วนบุคคลที่อยู่ในความควบคุมขององค์กร ไม่อยู่ในสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล จึงไม่ต้องจัดให้มีสัญญาประมวลผลข้อมูลส่วนบุคคลระหว่างกัน

4.2 การเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลของคู่สัญญาซึ่งเป็นบุคคลหรือนิติบุคคล เป็นไปตามคำสั่งหรือในนามผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ หากบุคคลหรือนิติบุคคลดังกล่าว เป็นผู้กำหนดวัตถุประสงค์การใช้ข้อมูลส่วนบุคคลเพื่อการให้บริการหรือการปฏิบัติตามสัญญาหรือข้อผูกพันที่มีอยู่กับองค์กร บุคคลหรือนิติบุคคล ซึ่งเป็นคู่สัญญาดังกล่าว ไม่อยู่ในสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ต้องจัดให้มีสัญญาประมวลผลข้อมูลส่วนบุคคล แต่อาจจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่ง

## 5. การดำเนินการกรณีองค์กรมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคล

### 5.1 การประเมินความพร้อมด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล

องค์กรจะต้องทำการตรวจสอบความพร้อมของบุคคลหรือนิติบุคคลซึ่งมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลที่องค์กรโอนข้อมูล เพื่อประมวลผลข้อมูลตามคำสั่งหรือในนามขององค์กร ว่ามีการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมีมาตรการรักษาความปลอดภัยเพียงพอตามมาตรฐานที่กฎหมายกำหนดหรือไม่

### 5.2 องค์กรกำหนดหน้าที่แก่ผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้

1) ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงบรรดานโยบายคุ้มครองข้อมูลส่วนบุคคล ประกาศความเป็นส่วนตัว ข้อตกลงหรือแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล หรือการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในการให้บริการและการปฏิบัติตามหน้าที่อื่น ๆ ของตนภายใต้สัญญาที่มีอยู่ทั้งหมด

2) ต้องแจ้งให้พนักงาน ตัวแทน บุคลากรของตนทราบ และดำเนินการให้แน่ใจว่าบุคคลเหล่านั้น ปฏิบัติตามคำสั่งของบริษัท และกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งหมดเท่านั้น

3) ต้องการประมวลผลข้อมูลส่วนบุคคลต้องทำภายใต้คำสั่งที่เป็นลายลักษณ์อักษรหรือมีบันทึกจากบริษัท เว้นแต่กรณีที่ผู้ให้บริการจะต้องปฏิบัติตามกฎหมาย

4) ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทั้งปวงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามสมควร

5) ต้องแจ้งให้บริษัททราบเป็นหนังสือทันทีโดยไม่ชักช้า เมื่อผู้ให้บริการทราบถึงกรณีดังต่อไปนี้

- การฝ่าฝืนอย่างร้ายแรงในการรักษาความปลอดภัยหรือมีเหตุที่น่าจะเชื่อได้ว่าข้อมูลส่วนบุคคลอาจถูกเปิดเผย เข้าถึง หรือใช้โดยไม่ได้รับอนุญาต รวมถึงมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- เมื่อมีคำร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- เมื่อมีหมายเรียก หรือคำสั่งจากศาล หรือเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐผู้มีอำนาจ หรือหน่วยงานกำกับดูแล เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

6) ต้องดำเนินการตามที่เหมาะสมและสมควร โดยค่าใช้จ่ายของผู้ประมวลผลข้อมูลส่วนบุคคล รวมไปถึงการแจ้งบุคคลที่ได้รับผลกระทบ การเยียวยาผลกระทบจากการที่ผู้ประมวลผลข้อมูลส่วนบุคคลไม่สามารถดำเนินการรักษาความปลอดภัย หรือป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตต่อข้อมูลส่วนบุคคลได้

7) ต้องไม่โอนข้อมูลส่วนบุคคลที่ได้รับมอบหมายให้ประมวลผลออกจาก หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากบุคคลอื่นที่อยู่นอกประเทศไทย โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลก่อน

8) ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเกิดกับผู้ควบคุมข้อมูลส่วนบุคคล และ/หรือผู้ประมวลผลข้อมูลส่วนบุคคล และ/หรือผู้ประมวลผลข้อมูลส่วนบุคคลต่าง ผู้ประมวลผลจะต้องดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และต้องแจ้งให้องค์กรรับทราบในทันที โดยไม่ชักช้า ภายในกำหนด ชั่วโมง นับแต่ทราบเหตุ บรรเทาความเสียหาย รวมไปถึงการให้ความช่วยเหลืออำนวยความสะดวกซึ่งกันและกัน

### 5.3 ข้อจำกัดการใช้และการเปิดเผย

1) ผู้ประมวลผลข้อมูลส่วนบุคคล ตกลงจะรักษาข้อมูลที่เป็นความลับทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลไว้เป็นความลับอย่างเคร่งครัด และจะใช้มาตรการที่จำเป็นตามสมควรเพื่อรักษาข้อมูลที่เป็นความลับ รวมทั้งปฏิบัติตามมาตรการรักษาความปลอดภัยทั้งหมดที่กำหนดขึ้น เพื่อป้องกันข้อมูลที่เป็นความลับจากการเข้าถึงหรือการใช้โดยไม่ได้รับอนุญาต

- เก็บรักษาข้อมูลที่เป็นความลับทั้งหมดภายในการควบคุมของคู่สัญญาฝ่ายนั้น ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องไม่ดำเนินการต่อไปนี้ โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคลก่อน

- เปิดเผยข้อมูลที่เป็นความลับดังกล่าวแก่บุคคลภายนอก (ที่ไม่ใช่หน่วยงานกำกับดูแลที่มีอำนาจเหนือผู้รับข้อมูล) เว้นแต่จะได้รับอนุญาตโดยประการอื่นภายใต้สัญญาที่มีอยู่

- ใช้ข้อมูลความลับดังกล่าว เพื่อวัตถุประสงค์ใด ๆ ที่นอกเหนือไปจากการใช้สิทธิหรือการปฏิบัติตามหน้าที่ผูกพันของตนภายใต้สัญญาที่มีอยู่

2) ผู้ประมวลผลข้อมูลส่วนบุคคล จะเปิดเผยข้อมูลที่เป็นความลับขององค์กรไม่ได้ เว้นแต่เฉพาะบุคคลหรือกรณีดังต่อไปนี้ให้แก่บุคลากรของตนที่เป็นพนักงาน ตัวแทน ที่จำเป็นต้องรู้ข้อมูลที่เป็นความลับดังกล่าวเพื่อใช้สิทธิของผู้รับข้อมูลดังกล่าว หรือเพื่อปฏิบัติตามหน้าที่ผูกพันของผู้รับข้อมูลดังกล่าวตามสัญญาที่มีอยู่ให้แก่หน่วยงานกำกับดูแล ที่มีอำนาจเหนือตามกฎหมายของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับอนุญาต โดยประการอื่นภายใต้สัญญาที่ตกลงร่วมกัน

3) ในการใช้ข้อมูลที่เป็นความลับข้างต้น ผู้ประมวลผลข้อมูลส่วนบุคคลต้องใช้ความพยายามตามสมควรในการค้นหาหรือป้องกันการใช้หรือการเปิดเผยข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต

4) ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบทันทีโดยไม่ชักช้า และจะให้ความร่วมมือในการขอคำสั่งยับยั้งการกระทำที่ฝ่าฝืนความลับของข้อมูลความลับจากหน่วยงานที่มีอำนาจ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบว่าหรือมีเหตุผลที่จะเชื่อได้ว่ามีบุคคลใด ๆ ที่ได้เข้าถึงข้อมูลที่เป็นความลับ โดยฝ่าฝืนหรือมีเจตนาที่จะฝ่าฝืนข้อกำหนดของสัญญาที่มีอยู่

5) นอกจากนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลอาจใช้หรือเปิดเผยข้อมูลที่เป็นความลับ (เว้นแต่ข้อมูลส่วนบุคคล) ตามกระบวนการทางกฎหมายที่กำหนดให้ต้องเปิดเผยข้อมูลที่เป็นความลับดังกล่าว โดยมีเงื่อนไขว่า ผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องใช้ความพยายามตามสมควรที่จะบอกกล่าวล่วงหน้าเป็นหนังสือเกี่ยวกับการถูกบังคับให้เปิดเผยดังกล่าว แก่องค์กร และจะต้องให้ความร่วมมือกับองค์กรในส่วนที่เกี่ยวข้องกับความพยายามใด ๆ ที่จะป้องกันหรือจำกัดขอบเขตของการเปิดเผยดังกล่าว

#### 5.4 มาตรการรักษาความปลอดภัย

การรักษาความมั่นคงปลอดภัย และความลับของข้อมูลส่วนบุคคล การเคหะแห่งชาติ ถือปฏิบัติตามนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ ซึ่งอ้างอิงตามมาตรฐานสากล ISO/IEC 27001 ในการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลส่วนบุคคล ซึ่งมีการทบทวนทุก ๆ ปี อย่างน้อยปีละ 1 ครั้ง

เพื่อประโยชน์ในการรักษาความลับและรักษาความปลอดภัยของข้อมูลส่วนบุคคล องค์กรและผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ดังนี้

1) กำหนดสิทธิในการเข้าถึงการใช้ การเปิดเผย การประมวลผลข้อมูลส่วนบุคคล รวมถึงการแสดงหรือยืนยันตัวบุคคลผู้เข้าถึงหรือใช้ข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความปลอดภัย รวมถึงกระบวนการทบทวนและการประเมินประสิทธิภาพของมาตรการรักษาความปลอดภัย ทั้งนี้ เป็นไปตามแนวนโยบายสารสนเทศขององค์กรอย่างเคร่งครัด

องค์กร จะเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลไว้เป็นอย่างดีตามมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อรักษาความปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมและเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล โดยองค์กรได้กำหนดนโยบาย ระเบียบ และหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลรวมถึงมาตรการเพื่อป้องกันไม่ให้ผู้รับข้อมูลไปจากองค์กรใช้หรือเปิดเผยข้อมูลนอกวัตถุประสงค์ หรือโดยไม่มีอำนาจ หรือโดยมิชอบ และองค์กรได้มีการปรับปรุงนโยบาย ระเบียบและหลักเกณฑ์ดังกล่าวเป็นระยะตามความจำเป็น และเหมาะสม นอกจากนี้ผู้บริหาร พนักงาน ผู้รับจ้าง ตัวแทน ที่ปรึกษา และผู้รับข้อมูลจากองค์กรมีหน้าที่ต้องรักษาความลับของข้อมูลส่วนบุคคลตามมาตรการรักษาความลับที่องค์กรกำหนด

2) ในกรณีที่มีการฝ่าฝืนมาตรการการรักษาความปลอดภัยขององค์กรจนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคลองค์กรจะดำเนินการแจ้งให้สำนักงานคณะกรรมการข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถทำได้ เว้นแต่การละเมิดนั้นมีความเสี่ยงที่จะกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลองค์กรจะดำเนินการแจ้งเหตุการละเมิดพร้อมทั้งแนวทางการเยียวยาให้เจ้าของข้อมูลทราบโดยไม่ชักช้า ทั้งนี้ องค์กรจะไม่รับผิดชอบในกรณีความเสียหายใดๆ อันเกิดจากการที่เจ้าของข้อมูลส่วนบุคคล

บุคคลหรือบุคคลอื่นซึ่งได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จงใจหรือประมาทเลินเล่อ หรือเพิกถอนตามมาตรการความปลอดภัยจนเป็นเหตุให้ข้อมูลส่วนบุคคลถูกใช้หรือเปิดเผยต่อบุคคลที่สามหรือบุคคลอื่นใด

องค์กรได้มีการทบทวนปรับปรุงขั้นตอนและมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรให้เป็นปัจจุบันสม่ำเสมอเพื่อให้ได้ระดับความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง และให้การรักษาความลับของข้อมูลส่วนบุคคล ความสมบูรณ์ ความพร้อมใช้งานและความคล่องตัวในการประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างต่อเนื่อง รวมทั้งการปกป้อง การสูญหายและการเก็บรวบรวม การเข้าถึง การใช้ การดัดแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ทั้งนี้ องค์กรจะนำมาตรการต่าง ๆ ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรมาใช้ในการประมวลผลข้อมูลส่วนบุคคลทุกประเภท ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะเป็นทางอิเล็กทรอนิกส์ หรือรูปแบบเอกสารก็ตาม

#### 5.5 การใช้หรือจ้างช่วงประมวลผลข้อมูลส่วนบุคคล

องค์กรไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลใช้หรือจ้างช่วงผู้ประมวลผลข้อมูลส่วนบุคคลอื่น เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรล่วงหน้าจากองค์กร

กรณีจ้างช่วงประมวลผลข้อมูล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีสัญญาที่กำหนดให้ผู้รับช่วง ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย เช่นเดียวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามสัญญาฉบับนี้ นอกจากนี้ผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลต้องรับประกันว่าจะใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามกฎหมายและมาตรการต้องให้ความคุ้มครองในระดับเดียวกับมาตรการที่ระบุตามนโยบายฉบับนี้

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่รับผิดชอบความเสียหายต่อองค์กร เมื่อผู้รับช่วงประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคลที่กำหนดตามนโยบายฉบับนี้

#### 6. การกำหนดความรับผิด

องค์กรกำหนดให้ผู้ประมวลผลจะต้องรับผิดชอบค่าใช้จ่ายให้กับองค์กรสำหรับค่าปรับ ความสูญเสีย หรือความเสียหายทั้งหมด อันเนื่องมาจากการที่ผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืนข้อกำหนดหรือเงื่อนไขใดๆ ภายใต้นโยบายฉบับนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 26 ธันวาคม พ.ศ. 2566



(นายทวีพงษ์ วิชัยดิษฐ)

ผู้ว่าการการเคหะแห่งชาติ