



การเคหะแห่งชาติ  
NATIONAL HOUSING AUTHORITY

คลองจั่น เขตบางกะปิ กทม. ๑๐๒๔๐ โทร ๐-๒๓๕๑-๗๗๗๗

## ประกาศการเคหะแห่งชาติ

### เรื่อง นโยบายการเปิดเผยและแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานภายนอก (Third Parties Data Transfer Policy)

การเคหะแห่งชาติ (“องค์กร”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล อันเป็นสิทธิขั้นพื้นฐานในความเป็นส่วนตัวของบุคคล โดยเจ้าของข้อมูลส่วนบุคคลย่อมมีความประสงค์ที่จะให้ข้อมูลของตนได้รับการดูแลให้มีความมั่นคงปลอดภัย เพื่อให้เจ้าของข้อมูลส่วนบุคคลเกิดความมั่นใจในการคุ้มครองข้อมูลส่วนบุคคล องค์กรจึงได้กำหนด นโยบายการเปิดเผยและแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานภายนอก (Third Parties Data Transfer Policy) (“นโยบาย”) ฉบับนี้ขึ้น เพื่อกำหนดแนวทางและรายละเอียดในการทำข้อตกลง ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดทำสัญญาการแลกเปลี่ยนข้อมูลส่วนบุคคล และนโยบายการเปิดเผยและแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานภายนอก แต่อย่างไรก็ตาม การจัดทำเอกสารดังกล่าว จะเป็นการเพิ่มมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้กับองค์กรเพิ่มมากขึ้น และเป็น การสร้างความเชื่อมั่นให้กับเจ้าของข้อมูลส่วนบุคคลว่าข้อมูลดังกล่าวจะถูกปกป้องและคุ้มครองอย่างปลอดภัย นโยบายการเปิดเผยและแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานภายนอกมีรายละเอียด ดังนี้

#### 1. วัตถุประสงค์

นโยบายการเปิดเผยและแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานภายนอก (Third Parties Data Transfer Policy) ฉบับนี้มีวัตถุประสงค์ ดังต่อไปนี้

- (1) เพื่อกำหนดบทบาทหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับการแบ่งปันข้อมูล
- (2) เพื่อกำหนดขั้นตอนหรือมาตรฐานการรักษาความมั่นคงปลอดภัยในการแบ่งปันข้อมูล
- (3) เพื่อกำหนดแนวทางในการปฏิบัติงานเมื่อมีการการแบ่งปันข้อมูล
- (4) เพื่อสร้างความเชื่อมั่นในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลต่อบุคคล

ลูกค้า คู่ค้า ผู้ใช้บริการ ตลอดจนบุคคลอื่นๆ ซึ่งมีส่วนได้เสียหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล เมื่อมีการแบ่งปันข้อมูลนั้น

#### 2. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ จะถูกนำมาบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลอื่น ที่ได้รับการแบ่งปันข้อมูลส่วนบุคคลจากองค์กร โดยผู้ควบคุมข้อมูลที่ได้รับการแบ่งปันข้อมูลนั้น มีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

### 3. คำนิยาม

“สัญญาแบ่งปันข้อมูลส่วนบุคคล” หมายความว่า สัญญาแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) คือ สัญญาเพื่อใช้เป็นหลักฐานการแบ่งปันข้อมูลส่วนบุคคลระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล อาทิ การจำกัดวัตถุประสงค์ ความสมบูรณ์และความลับ โดยรายละเอียดในสัญญาแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) ประกอบด้วย (1) ข้อมูลส่วนบุคคลที่คู่สัญญาแบ่งปันกัน และ (2) ฐานกฎหมายในการแบ่งปันข้อมูลส่วนบุคคล โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลทั้ง 2 ฝ่าย ต้องมีการรับทราบและตกลงว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของข้อมูลส่วนบุคคลที่ตนประมวลผล พร้อมแจ้งข้อมูลที่เกี่ยวข้องกับการแบ่งปันข้อมูลและขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือมีฐานกฎหมายหรืออำนาจหน้าที่โดยชอบด้วยกฎหมายให้สามารถเปิดเผยข้อมูลส่วนบุคคลให้อีกฝ่าย

“องค์กร” หมายความว่า การเคหะแห่งชาติ

“บุคคล” หมายความว่า บุคคลธรรมดา

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม องค์กรอาจเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่ได้รับจากเจ้าของข้อมูลโดยตรง (เช่น แพลตฟอร์มลงทะเบียนขององค์กร) หรือได้รับหรือเข้าถึงได้จากแหล่งอื่น (เช่น กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ กรมการปกครอง กระทรวงมหาดไทย กรมการกงสุล กระทรวงการต่างประเทศ องค์กรข้อมูลเครดิต กรมบังคับคดี สถาบันการเงิน ที่ปรึกษาทางวิชาชีพ สื่อสังคม แพลตฟอร์มออนไลน์ของบุคคลภายนอก หรือแหล่งข้อมูลสาธารณะอื่น ๆ) หรือผ่านองค์กรในเครือผู้ให้บริการ พันธมิตรทางธุรกิจ หน่วยงานทางการ หรือบุคคลภายนอก

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

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลนี้จะหมายถึงบุคคลธรรมดาเท่านั้น และไม่รวมถึง “นิติบุคคล” ที่จัดตั้งขึ้นตามกฎหมาย เช่น องค์กรสมาคม มูลนิธิ หรือองค์กรอื่นใด

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า บุคคลซึ่งองค์กรแต่งตั้งให้ทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

### 4. เกณฑ์การพิจารณาการจัดทำ

องค์กรจะมีการจัดทำสัญญาแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) เมื่อมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลอื่น โดยจะแนบกับสัญญาหลักที่ทำกับผู้ควบคุมข้อมูลอื่นอาจจะอยู่ในเนื้อหาสัญญาก็ได้

## 5. วิธีการดำเนินการกับข้อมูลที่มีการเผยแพร่ทางชาติจะแบ่งปันแก่ผู้ควบคุมข้อมูลอื่น

5.1 การกำหนดข้อมูลที่จะแลกเปลี่ยน องค์กรจะกำหนดข้อมูลที่จะแลกเปลี่ยนกับผู้ควบคุมข้อมูลอีกฝ่ายหนึ่งที่ได้รับการแบ่งปันข้อมูลส่วนบุคคล โดยจะแบ่งปันข้อมูลเท่าที่จำเป็น เพื่อปฏิบัติตามสัญญาหรือฐานทางกฎหมายอื่น ๆ ที่เกี่ยวข้องที่ให้อำนาจในการแบ่งปันข้อมูลส่วนบุคคล โดยข้อมูลที่ต้องกรเก็บมานั้น องค์กรจะกระทำโดยชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ ในการเก็บรวบรวม จะเก็บโดยขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะที่มีการเก็บข้อมูล เว้นแต่มีฐานทางกฎหมายอื่นรองรับที่องค์กรไม่ต้องขอความยินยอม และองค์กรจะแจ้งรายละเอียดเกี่ยวกับการเก็บข้อมูลนั้น ตามมาตรา 23 เมื่อมีการเก็บข้อมูลจากเจ้าของข้อมูล

5.2 การแลกเปลี่ยนข้อมูลกับผู้ควบคุมข้อมูลอื่น องค์กรจะกำหนดวัตถุประสงค์เท่าที่จำเป็นในการแลกเปลี่ยนข้อมูล ตามหลักการประมวลผลเท่าที่จำเป็น ตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมหรือตามฐานกฎหมายอื่นไว้ และในกรณีที่องค์กรเปิดเผยแก่บุคคลภายนอกเกินวัตถุประสงค์ องค์กรจะทำการขอความยินยอมจากเจ้าของข้อมูลก่อนมีการเปิดเผยหรือ แลกเปลี่ยน หรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลที่มีการแบ่งปันข้อมูล

(1) การเปิดเผยข้อมูลนั้น องค์กรจะเก็บโดยอาศัยฐานความยินยอมหรือฐานทางกฎหมายอื่นโดยจะแจ้งให้เจ้าของข้อมูลทราบก่อนหรือขณะที่มีการเก็บข้อมูล

(2) องค์กรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับการแบ่งปันข้อมูลนั้น ต้องให้ความสำคัญและรับผิดชอบในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามนโยบายอย่างเคร่งครัด โดยมีรายละเอียดดังนี้

หน้าที่	รายละเอียด
1.เก็บรวบรวม ใช้ เปิดเผยให้เป็นไปตามกฎหมาย	การเก็บรวบรวม ใช้ เปิดเผย ต้องมีฐานทางกฎหมายรองรับ ดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ และต้องดำเนินการเก็บรวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้น ซึ่งเกี่ยวข้องกับหน้าที่ในการจัดเตรียมเอกสารต่าง ๆ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมั่นใจว่า หากยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลเข้าไปเก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอย่างไร
2.เปิดช่องให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมาย	บันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เมื่อผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมระบุเหตุผลในรายการบันทึกการปฏิบัติตามมาตรา 39
3.จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล	เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเป็นไปตามมาตรฐานขั้นต่ำ
4.จัดให้มีมาตรการป้องกันการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ	ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น มีการโอนข้อมูลส่วนบุคคลให้ผู้ประมวลผล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจหรือโดยไม่ถูกต้องตามกฎหมาย
5.จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย	จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็น

หน้าที่	รายละเอียด
หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้	ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย
6.แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	ต้องแจ้งเหตุละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่เมื่อทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า
7.หน้าที่ในการจัดทำบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities : RoPA)	ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์

## 6. มาตรการรักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัย และความลับของข้อมูลส่วนบุคคล การเคหะแห่งชาติ ถือปฏิบัติตามนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสำหรับสารสนเทศของการเคหะแห่งชาติ ซึ่งอ้างอิงตามมาตรฐานสากล ISO/IEC 27001 ในการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลส่วนบุคคล ซึ่ง มีการทบทวนทุก ๆ ปี อย่างน้อยปีละ 1 ครั้ง โดยมีมาตรการดังนี้

6.1 กำหนดสิทธิในการเข้าถึงการใช้ การเปิดเผย การประมวลผลข้อมูลส่วนบุคคล รวมถึง การแสดงหรือยืนยันตัวบุคคลผู้เข้าถึงหรือใช้ข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความปลอดภัย รวมถึง กระบวนการทบทวนและการประเมิน ประสิทธิภาพของมาตรการรักษาความปลอดภัย ทั้งนี้เป็นไปตาม แผนนโยบายสารสนเทศขององค์กรอย่างเคร่งครัด

องค์กรจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้เป็นอย่างดีตามมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อรักษาความปลอดภัย ในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล โดยองค์กรได้ กำหนดนโยบาย ระเบียบ และหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมาตรการเพื่อป้องกันไม่ให้ ผู้รับข้อมูลไปจากองค์กรใช้ หรือเปิดเผยข้อมูลนอกวัตถุประสงค์ หรือโดยไม่มีอำนาจหรือโดยมิชอบ และองค์กร ได้มีการปรับปรุงนโยบาย ระเบียบและหลักเกณฑ์ดังกล่าวเป็นระยะตามความจำเป็น และเหมาะสม นอกจากนี้ ผู้บริหาร พนักงาน ผู้รับจ้าง ตัวแทน ที่ปรึกษา และผู้รับข้อมูลจากองค์กรมีหน้าที่ต้องรักษาความลับของ ข้อมูลส่วนบุคคลตามมาตรการรักษาความลับที่องค์กรกำหนด

6.2 ในกรณีที่มีการฝ่าฝืนมาตรการรักษาความปลอดภัยขององค์กรจนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล องค์กรจะดำเนินการแจ้งให้สำนักงานคณะกรรมการข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถทำได้ เว้นแต่การละเมิดนั้นมีความเสี่ยงที่จะกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรจะดำเนินการแจ้งเหตุการละเมิดพร้อมทั้งแนวทางการเยียวยาให้เจ้าของข้อมูลทราบโดยไม่ชักช้า ทั้งนี้ องค์กรจะไม่รับผิดชอบในกรณีความเสียหายใดๆ อันเกิดจากการที่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น ซึ่งได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลลงใจหรือประมาทเลินเล่อหรือเพิกถอนตามมาตรการความปลอดภัยจนเป็นเหตุให้ข้อมูลส่วนบุคคลถูกใช้หรือเปิดเผยต่อบุคคลที่สามบุคคลอื่นใด

องค์กรได้มีการทบทวน ปรับปรุงขั้นตอนและมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรให้เป็นปัจจุบันสม่ำเสมอ เพื่อให้ได้ระดับความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง และให้การรักษาความลับของข้อมูลส่วนบุคคล ความสมบูรณ์ ความพร้อมใช้งานและความคล่องตัวในการประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างต่อเนื่อง รวมทั้งการปกป้อง การสูญหายและการเก็บรวบรวมการเข้าถึง การใช้ การดัดแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ทั้งนี้ องค์กรจะนำมาตรการต่าง ๆ ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรมาใช้ในการประมวลผลข้อมูลส่วนบุคคลทุกประเภท ไม่ว่าจะเป็นการประมวลผลข้อมูลส่วนบุคคลนั้นจะเป็นทางอิเล็กทรอนิกส์ หรือรูปแบบเอกสารก็ตาม

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 26 ธันวาคม พ.ศ. 2566



(นายทองชัย วิชัยดิษฐ์)

ผู้ว่าการการเคหะแห่งชาติ