

(ร่าง) ข้อตกลงการประมวลผลข้อมูล
(Data Processing Agreement)

ตามสัญญาเลขที่ ลงวันที่ โครงการ

ฉบับที่ 1

- ข้อตกลงให้ประมวลผลข้อมูลนี้มีขอบเขตการบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคลของผู้ใช้บริการ
- ข้อตกลงนี้ถือเป็นส่วนหนึ่งของสัญญาการให้บริการหลัก
- ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสาม

1. ความสัมพันธ์ระหว่างคู่สัญญา

1.1 สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (“ผู้ให้บริการ”)

ผู้ให้บริการจะอยู่ในฐานะผู้ควบคุมข้อมูลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ให้บริการในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการควบคุมข้อมูลที่มีผลใช้บังคับกับกรณี

1.2 [ชื่อของผู้ประมวลผลข้อมูล] (“ผู้ให้บริการ”)

ผู้ให้บริการจะอยู่ในฐานะของผู้ประมวลผลข้อมูลตลอดระยะเวลาของสัญญาการให้บริการหลัก โดยผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลมีหน้าที่ต้องปฏิบัติตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลที่มีผลใช้บังคับกับกรณี

2. คำนิยาม

“สัญญาการให้บริการหลัก”	หมายถึง	[สัญญาการให้บริการหลัก] ระหว่าง สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และ [ชื่อของผู้ประมวลผลข้อมูล] ลงวันที่ [•]
“ข้อตกลง”	หมายถึง	ข้อตกลงให้ประมวลผลข้อมูลฉบับนี้
“กฎหมายคุ้มครองข้อมูลส่วนบุคคล”	หมายถึง	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศหรือกฎเกณฑ์ที่เกี่ยวข้อง
“ข้อมูลส่วนบุคคล”	หมายถึง	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“เจ้าของข้อมูล”	หมายถึง	บุคคลธรรมดาซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคล ไม่ว่าจะโดยทางตรงหรือทางอ้อม และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ และผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ
“ประมวลผลข้อมูล”	หมายถึง	การเก็บรวบรวม การใช้ การเปิดเผย การลบ การทำลาย ข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล
“ละเมิดข้อมูลส่วนบุคคล”	หมายถึง	การรั่วไหล หรือการละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลซึ่งทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง ไม่ว่าจะโดยอุบัติเหตุหรือโดยมิชอบ ด้วยกฎหมาย รวมถึงการเปิดเผย, เข้าถึง, เก็บรวบรวม หรือประมวลผลข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับอนุญาต

3. ประเภทของข้อมูลส่วนบุคคล

- 3.1 ผู้ใช้บริการตระหนักและยอมรับว่าการใช้บริการตามสัญญาการให้บริการหลัก ถือเป็นคำสั่งให้ผู้ใช้บริการอาจทำการประมวลผลข้อมูลส่วนบุคคลที่จำเป็นสำหรับการบริการที่กำหนดไว้ในสัญญาการให้บริการหลัก
- 3.2 ผู้ใช้บริการยอมรับว่าการประมวลผลข้อมูลส่วนบุคคลของผู้ให้บริการประกอบด้วยข้อมูลส่วนบุคคลดังต่อไปนี้ ไม่ว่าจะทั้งหมดหรือเพียงบางส่วน

รายการข้อมูลส่วนบุคคล
[โปรดระบุประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น ชื่อ-นามสกุล ที่อยู่ อีเมล]

4. หน้าที่ในการประมวลผลข้อมูล

4.1 ผู้ให้บริการจะทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่เป็นลายลักษณ์อักษรจากผู้ให้บริการ อันได้แก่ การประมวลผลข้อมูลตามวัตถุประสงค์ดังต่อไปนี้เท่านั้น เว้นแต่จะมีคำสั่งจากผู้ให้บริการให้ประมวลผลข้อมูลเพิ่มเติม ตามข้อ 4.2

ชื่อกิจกรรม (รหัสกิจกรรมตาม ROP (ROP ID))	วัตถุประสงค์	รายการข้อมูลส่วนบุคคล
[โปรดระบุ]	[โปรดระบุ]	[โปรดระบุ]

- 4.2 ผู้ให้บริการอาจมีคำสั่งเป็นลายลักษณ์อักษรให้ผู้ให้บริการประมวลผลข้อมูลเพิ่มเติม โดยผู้ให้บริการจะทำการประมวลผลข้อมูลดังกล่าวโดยพลัน
- 4.3 ในกรณีที่ผู้ให้บริการพิจารณาแล้วเห็นว่า การออกคำสั่งตามข้อ 4.1 และ 4.2 ของผู้ให้บริการนั้น เป็นการออกคำสั่งที่ละเมิดต่อกฎหมาย ผู้ให้บริการจะทำการแจ้งผู้ให้บริการโดยพลัน แต่ทั้งนี้ ผู้ให้บริการตระหนักและยอมรับว่า ผู้ให้บริการไม่ได้มีหน้าที่ให้คำปรึกษาทางกฎหมายใด ๆ แก่ผู้ให้บริการ
- 4.4 ผู้ให้บริการจะต้องประมวลผลข้อมูลโดยชอบด้วยกฎหมาย เป็นธรรม และมีความโปร่งใส
- 4.5 ผู้ให้บริการจะประมวลผลข้อมูลส่วนบุคคลเฉพาะที่เกี่ยวข้องและจำเป็นต่อการให้บริการเท่านั้น
- 4.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการหรือเจ้าหน้าที่ที่เกี่ยวข้องจะต้องปฏิบัติตามหน้าที่เพื่อช่วยเหลือและให้คำแนะนำเกี่ยวกับการดำเนินการของผู้ให้บริการให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5. การรักษาความลับของข้อมูล

- 5.1 ผู้ให้บริการจะใช้ความพยายามตามสมควรให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะ บุคลากร หรือบุคคลที่ได้รับมอบหมายที่มีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์ของสัญญาการให้บริการหลัก
- 5.2 ผู้ให้บริการจะดำเนินการให้บุคลากร หรือบุคคลที่ได้รับมอบหมายตามข้อ 5.1 มีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงไม่เปิดเผยข้อมูลเป็นลายลักษณ์อักษร
- 5.3 บรรดาเอกสาร ข้อมูล และสื่อบันทึกข้อมูล ซึ่งใช้กับเครื่องคอมพิวเตอร์ รวมทั้งข้อมูลอื่น ๆ ที่ได้จากการปฏิบัติราชการ ให้ถือว่าเป็นความลับของทางราชการ ผู้ให้บริการต้องรักษาไว้เป็นความลับโดยเคร่งครัด

- 5.4 ผู้ให้บริการ ต้องรักษาความลับของทางราชการ อาทิ รายการ และ/หรือรายละเอียด และ/หรือภาพ และ/หรือข้อมูลใดๆ ที่เกี่ยวข้องกับบุคลากร การบัญชี การเงิน รายการทรัพย์สิน กรรมวิธี ข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติงานทั้งหมด อันจะส่งผลให้เกิดความเสียหายกับผู้ให้บริการ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้บริการแล้วเท่านั้น
- 5.5 ผู้ให้บริการ จะปฏิบัติตามระเบียบต่าง ๆ ที่ผู้ให้บริการกำหนด และ/หรือจะได้กำหนดขึ้นต่อไป ในภายหน้าอย่างเคร่งครัด และหากผู้ให้บริการเปิดเผยข้อมูลตลอดจนเอกสารอันเป็นความลับของทางราชการผู้ให้ข้อตกลงต้องรับผิดชอบในความเสียหายที่เกิดขึ้นทั้งสิ้น

6. มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

- 6.1 ผู้ให้บริการมีหน้าที่จะต้องจัดให้มีและธำรงรักษาไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิค ทั้งนี้ มาตรการข้างต้นจะต้องคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในสัญญา โดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

7. สิทธิของเจ้าของข้อมูล

- 7.1 ผู้ให้บริการจะสนับสนุนให้ผู้ให้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ โดยจัดให้มีมาตรการทั้งเชิงองค์กรและเชิงเทคนิค เพื่อให้ผู้ให้บริการสามารถตอบสนองต่อคำร้องขอของเจ้าของข้อมูล อันเป็นการใช้สิทธิของเจ้าของข้อมูลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล
- 7.2 ในกรณีที่ผู้ให้บริการได้รับคำร้องขอจากเจ้าของข้อมูลซึ่งได้ระบุว่าผู้ให้บริการนั้นเป็นผู้ควบคุมข้อมูล ผู้ให้บริการจะทำการส่งคำร้องขอนั้นต่อไปยังผู้ให้บริการ ภายใน [ระบุระยะเวลา เช่น 3 วัน] ทั้งนี้ ผู้ให้บริการจะไม่ทำการตอบสนองต่อคำร้องดังกล่าวโดยปราศจากการหารือกับผู้ให้บริการ

8. การถ่ายโอนข้อมูลส่วนบุคคล

- 8.1 ภายในบังคับของข้อ 8.2 ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการตามสัญญา การให้บริการหลักจะถูกเก็บรักษาในภูมิภาคที่กำหนดไว้ในสัญญาการให้บริการหลัก หรือที่ผู้ให้บริการกำหนดเป็นลายลักษณ์อักษร โดยผู้ให้บริการจะไม่ทำการโอนถ่ายข้อมูลส่วนบุคคลไปยังภูมิภาคอื่น เว้นแต่ จะได้รับคำอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้บริการ
- 8.2 ในกรณีมีความจำเป็นเพื่อให้บริการและเป็นกรณีที่ได้รับความสั่งให้ประมวลผลข้อมูลส่วนบุคคลจากผู้ให้บริการเป็นลายลักษณ์อักษรแล้ว ผู้ให้บริการสามารถเข้าถึงและประมวลผลข้อมูลส่วนบุคคลจากพื้นที่หรือตำแหน่งนอกภูมิภาคที่กำหนดในข้อ 8.1 ได้

9. การประมวลผลข้อมูลช่วง

- 9.1 ห้ามมิให้ผู้ให้บริการเปลี่ยนตัว หรือมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (ไม่ว่าจะกี่ทอดก็ตาม) ทำการประมวลผลข้อมูลตามที่กำหนดในข้อตกลงนี้แทน เว้นแต่จะได้รับอนุญาตจากผู้ใช้บริการเป็นลายลักษณ์อักษรเป็นการเฉพาะ
- 9.2 ผู้ประมวลผลข้อมูลช่วงที่ได้รับอนุญาตจากผู้ใช้บริการตามข้อ 9.1 จะต้องทำข้อตกลงประมวลผลช่วงเป็นลายลักษณ์อักษรกับผู้ใช้บริการ โดยข้อตกลงประมวลผลช่วงจะต้องกำหนดภาระหน้าที่ของผู้ประมวลผลช่วง เช่นเดียวกับภาระหน้าที่ของผู้ให้บริการตามภายใต้ข้อตกลงนี้
- 9.3 ผู้ให้บริการไม่หลุดพ้นจากความรับผิดชอบตามข้อตกลงนี้ต่อผู้ใช้บริการ ในกรณีที่ผู้ประมวลผลช่วงไม่ปฏิบัติตามที่ตามสัญญาประมวลผลช่วงในข้อ 9.2

10. การแจ้งเตือนหากเกิดเหตุละเมิดข้อมูลส่วนบุคคล

- 10.1 ผู้ให้บริการและบุคลากรของผู้ให้บริการมีหน้าที่ทำการประเมินและตอบสนองต่อการกระทำใด ๆ ซึ่งอาจมีลักษณะเป็นการละเมิดข้อมูลส่วนบุคคล
- 10.2 ในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคลซึ่งอยู่ในความรับผิดชอบของผู้ให้บริการภายใต้ข้อตกลงนี้ ผู้ให้บริการจะจัดให้มีมาตรการที่เหมาะสมเพื่อระงับสาเหตุของการละเมิดข้อมูลส่วนบุคคล และเพื่อป้องกันมิให้เกิดเหตุดังกล่าวขึ้นอีก
- 10.3 ผู้ให้บริการจะทำการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อผู้ใช้บริการโดยไม่ชักช้า ภายในระยะเวลา 24 ชั่วโมง นับตั้งแต่ได้ทราบถึงเหตุละเมิดที่เกิดขึ้น โดยในการแจ้งนั้น ผู้ให้บริการจะให้ข้อมูลแก่ผู้ใช้บริการภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด ดังต่อไปนี้
 - คำอธิบายลักษณะของเหตุละเมิดข้อมูลส่วนบุคคล
 - ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิดที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการ (หากเป็นไปได้)
 - จำนวนข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่เกี่ยวข้อง
 - ระยะเวลาที่เกิดการละเมิดข้อมูลส่วนบุคคล นับแต่ทราบเหตุละเมิดข้อมูลส่วนบุคคล
 - คำอธิบายเกี่ยวกับมาตรการในการรับมือกับเหตุละเมิดข้อมูลส่วนบุคคลที่ได้ดำเนินการไปแล้ว เพื่อลดผลกระทบของเหตุละเมิด

11. การตรวจสอบ

- 11.1 ผู้ให้บริการจะต้องชี้แจงข้อมูลที่จำเป็นตามที่ผู้ใช้บริการร้องขอ เพื่อแสดงให้เห็นว่าผู้ให้บริการปฏิบัติตามข้อตกลงนี้
- 11.2 ผู้ให้บริการจะอนุญาตและให้ความร่วมมือกับผู้ใช้บริการ หรือบุคคลที่ได้รับมอบหมาย ในการตรวจสอบข้อมูลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้

12. การลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

เมื่อการให้บริการตามสัญญาให้บริการหลักสิ้นสุดลง ผู้ให้บริการมีหน้าที่ลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ให้แก่ผู้ใช้บริการภายใน [ระบุระยะเวลา เช่น ๗ วัน] โดยผู้ให้บริการจะต้องส่งหนังสือแจ้งและรับรองไปยังผู้ใช้บริการ เป็นลายลักษณ์อักษรว่าได้ดำเนินการลบทำลาย หรือส่งคืนข้อมูลส่วนบุคคลเป็นที่เรียบร้อยแล้ว ให้แก่ผู้ใช้บริการทราบภายใน [ระบุระยะเวลา เช่น ๗ วัน] นับแต่ผู้ให้บริการได้พ้นจากภาระผูกพันและความรับผิดชอบที่ปวงตามสัญญาแล้ว

[•] โดย

[•] โดย

ลงชื่อ.....ผู้ใช้บริการ
([•])

ลงชื่อ.....ผู้ให้บริการ
([•])

ลงชื่อ.....พยาน
([•])

ลงชื่อ.....พยาน
([•])