ข้อตกลงการประมวลข้อมูลส่วนบุคคล

ข้อตกลงฉบับนี้ทำขึ้น ณ เมื่อวันที่ โดยมีผลบังคับใช้ตั้งแต่วันที่

**ระหว่าง:**

บริษัท XXXX จดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย โดยมีทะเบียนนิติบุคคลเลขที่ XXXXXX และมีสำนักงานตั้งอยู่ XXXXX ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า **“ผู้ควบคุมข้อมูลส่วนบุคคล”** หรือ “XXX” ฝ่ายหนึ่ง กับ

บริษัท ตั้งอยู่เลขที่ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “**ผู้ประมวลผลข้อมูลส่วนบุคคล**” หรือ “บริษัทฯ” โดยทั้งสองฝ่ายตกลงกันดังต่อไปนี้

1. **วัตถุประสงค์**

XXXXXX ได้ติดต่อและ/หรือ ว่าจ้าง บริษัทฯ เพื่อ  นั้น XXXXXX อาจมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการดำเนินงานตามเอกสารแนบท้าย 1 ให้แก่บริษัทฯ XXXXXX จึงประสงค์ให้บริษัทฯ เก็บรักษาข้อมูลดังกล่าวตามมาตรฐานความปลอดภัยในระดับเดียวกันโดยให้เป็นไปตามที่กฎหมายกำหนดทั้งในขณะนี้และภายภาคหน้า

1. **ข้อมูลส่วนบุคคล**

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

1. **การประมวลข้อมูลส่วนบุคคล**

การประมวลผลข้อมูลส่วนบุคคลในข้อตกลงฉบับนี้ หมายถึง การเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล โดยผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะประมวลผลข้อมูลส่วนบุคคลตามเงื่อนไขดังนี้

* 1. ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ระบุในข้อ 1 เท่านั้น
  2. ห้ามเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอก เว้นแต่จะเป็นการเปิดเผยข้อมูลส่วนบุคคลให้แก่ลูกจ้างหรือพนักงานของผู้ประมวลผลข้อมูลที่เกี่ยวข้องโดยตรงกับการดำเนินงานตามวัตถุประสงค์ในข้อ 1
  3. ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ทำซ้ำข้อมูลส่วนบุคคลแม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลส่วนบุคคลให้บรรลุวัตถุประสงค์ตามที่กำหนดไว้ในข้อ 1
  4. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องกำกับดูแลการปฏิบัติหน้าที่ของพนักงาน ลูกจ้าง ตัวแทน และ/หรือผู้รับจ้างของผู้ประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามที่ XXXXXX กำหนด และบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามที่กฎหมายกำหนดทั้งในขณะปัจจุบันและในภายภาคหน้า
  5. กรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลได้โอนกิจการ รวมกิจการ หรือควบกิจการ หรือดำเนินการอื่น ๆ ในลักษณะที่มีการเปลี่ยนแปลงอำนาจในการดำเนินกิจการของผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแจ้งให้ XXXXXX ทราบทันทีโดยข้อตกลงฉบับนี้ยังคงมีผลผูกพันผู้ประมวลผลข้อมูลส่วนบุคคลและผู้รับโอนสิทธิของผู้ประมวลผลข้อมูลส่วนบุคคลด้วย

**4. มาตรการรักษาความปลอดภัย**

* 1. ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการจัดหามาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ พิจารณาถึงความก้าวหน้าทางเทคโนโลยี ค่าใช้จ่ายในการดำเนินการ ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูล
  2. หากการกระทำใดของผู้ประมวลผลข้อมูลทำให้เกิดข้อพิพาทหรือความเสียหายแก่ XXXXXX ผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

**5. สิทธิของเจ้าของข้อมูลส่วนบุคคล**

* 1. ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อช่วยเหลือหรือสนับสนุนผู้ควบคุมข้อมูลส่วนบุคคลสามารถตอบสนองตามคำร้องของเจ้าของข้อมูลส่วนบุคคลอันเป็นการใช้สิทธิของเจ้าของส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้ยื่นมายัง XXXXX
  2. ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งต่อผู้ควบคุมข้อมูลส่วนบุคคล ในกรณีที่คำร้องเกี่ยวกับข้อมูลส่วนบุคคลซึ่งยื่นโดยเจ้าของข้อมูลส่วนบุคคล

**6. การแจ้งเตือน**

* 1. หากเกิดการละเมิดข้อมูลส่วนบุคคลซึ่งเกิดจากอุบัติเหตุ การทำลาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้ประมวลผลต้องดำเนินการแจ้งให้ XXXXXX รู้โดยทันทีหรือไม่เกิน 24 ชั่วโมงหลังจากรับทราบเหตุ
  2. ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้มาตรการตามที่เห็นสมควร ในการระบุถึงสาเหตุของการละเมิดและการป้องกันปัญหาดังกล่าวไม่ให้เกิดซ้ำ และจะให้ข้อมูลให้แก่ XXXX ภายใต้ขอบเขตที่กฎหมายกำหนดดังต่อไปนี้
     1. รายละเอียดของลักษณะและผลที่อาจเกิดขึ้นของการละเมิด
     2. มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด
     3. ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลซึ่งถูกละเมิด
     4. ข้อมูลอื่นๆ ที่เกี่ยวข้องกับการละเมิด

**7. การลบและการเก็บรักษาข้อมูลส่วนบุคคล**

“การลบ” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกจากระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใดๆ

* 1. เก็บรักษาข้อมูลส่วนบุคคลในสถานที่ ระบบ หรือฐานข้อมูลที่มีการจำกัดการเข้าถึงเฉพาะผู้เกี่ยวข้องเท่านั้น
  2. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องส่งคืนข้อมูลส่วนบุคคล รวมถึงสำเนาของข้อมูล (หากมี) ให้แก่ XXXXXX ภายในระยะเวลา 7 วัน นับตั้งแต่วันที่สัญญาสิ้นสุดลง หรือนับแต่วันที่ XXXXXX มีหนังสือแจ้งอย่างเป็นทางการไปยังผู้ประมวลผลข้อมูลส่วนบุคคลให้ส่งคืนหรือทำลายสำเนาข้อมูลส่วนบุคคล
  3. ทำลายข้อมูลหลังจากบรรลุวัตถุประสงค์ตามข้อ 1 เมื่อหมดระยะเวลาสัญญาที่มีต่อกัน หรือเมื่อXXXXXX มีหนังสือแจ้งอย่างเป็นทางการไปยังผู้ประมวลข้อมูลส่วนบุคคลตามวิธีการที่ XXXXXXกำหนด
  4. ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคล และแจ้งให้  
     XXXXXXXX ทราบถึงนโยบายดังกล่าว โดยนโยบายเกี่ยวกับการลบข้อมูลส่วนบุคคลดังกล่าวจะมีเนื้อหาที่ครอบคลุมถึงระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลด่อนที่จะถูกลบหลังจากการยกเลิกข้อตกลงการประมวลผลข้อมูลส่วนบุคล ทั้งนี้ เพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลมิให้สูญเสียข้อมูลส่วนบุคคลของตนไปโดยอุบัติเหตุเพราะเหตุที่ข้อตกลงสิ้นสุด

**8. การส่งหรือโอนข้อมูล**

* 1. ห้ามมิให้ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศหรือองค์การระหว่างประเทศ เว้นแต่จะได้รับความยินยอมจาก XXXXXXXX เป็นลายลักษณ์อักษร
  2. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ จะต้องเป็นไปตามเงื่อนไขที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบบุคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง

ข้อตกลงฉบับนี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความในข้อตกลงโดยละเอียดแล้ว จึงได้ลงลายมือชื่อพร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญ ต่อหน้าพยาน และต่างเก็บรักษาไว้ฝ่ายละหนึ่งฉบับ

|  |
| --- |
| บริษัท XXXX จำกัด (มหาชน) |
| ลงชื่อ ( ) ตำแหน่ง  พยาน    ( ) |

|  |
| --- |
| บริษัท |
| ลงชื่อ ( ) ตำแหน่ง  พยาน    ( ) |

**เอกสารแนบท้าย ๑**

**รายละเอียดการประมวลผลข้อมูลส่วนบุคคล (ตัวอย่างเบื้องต้นสำหรับ Healthcare)**

รายละเอียดเกี่ยวกับข้อตกลงการประมวลผลข้อมูลส่วนบุคคล:

จัดจ้างผู้ประมวลผลข้อมูลส่วนบุคคล\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล:

1. บริการเว็บไซด์เพื่อนัดหมายแพทย์, การพูดคุย หรือปรึกษาสุขภาพกับแพทย์, จัดหาห้องพัก, จัดหารถพยาบาลการซื้อบริการหรือสินค้าของโรงพยาล, ลูกค้าสัมพันธ์, สำรวจความพึงพอใจของผู้ใช้บริการ, ระบบสมาชิกบนเว็บไซด์, การรับข้อร้องเรียน ปัญหาการใช้บริการ, การรับข้อมูลข่าวสาร
2. การส่งข้อความแจ้งเตือนการนัดหมายแพทย์, การเสนอความช่วยเหลือ, ข่าวสารจากผู้ควบคุมข้อมูลส่วนบุคคล
3. บริการ Call Center เพื่อรับข้อร้องเรียน, การซื้อบริการหรือสินค้า, ลูกค้าสัมพันธ์, ติดตามผลการให้บริการ
4. ประมวลผลด้านการตลาด การส่งเสริมการขาย และลูกค้าสัมพันธ์
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ประเภทข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

1. *ข้อมูลซึ่งระบุถึงตัวตน และช่องทางการติดต่อ ได้แก่ ชื่*อ - *นามสกุล อายุ วันเกิด เพศ เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง ลายมือชื่อ ภาพถ่ายใบหน้า หมายเลขโทรศัพท์ อีเมล ที่อยู่*
2. *ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ*
3. *ข้อมูลทางการเงิน เช่น ข้อมูลบัญชีธนาคาร สำเนาสมุดบัญชี ข้อมูลบัตรเครดิตหรือเดบิต*
4. *ข้อมูลสถิติ เช่น จำนวนผู้ป่วย*
5. ข้อมูลการเข้ารับบริการ เช่น ข้อมูลการนัดหมายแพทย์ ข้อมูลส่วนบุคคลของญาติ ความต้องการเกี่ยวกับห้องพัก อาหาร และบริการเสริมอื่นๆ
6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*ข้อมูลอ่อนไหว*

1. *ข้อมูลชีวภาพ เช่น หมู่เลือด ผลการทบสอบจากห้องทดลอง*
2. *ข้อมูลทางการแพทย์ เช่น รายงานที่เกี่ยวกับสุขภาพกายและสุขภาพจิต การใช้ยาและการแพ้ยา*
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_