ข้อตกลงการประมวลผลข้อมูล

https://scratcher.io/th/data-processing-agreement

เวอร์ชันมาตรฐาน อัปเดตล่าสุดเมื่อ 22 ตุลาคม 2026 ข้อตกลงการประมวลผลข้อมูลฉบับนี้เป็นส่วนหนึ่งของข้อตกลงระหว่างคุณกับ Scratcher ApS (CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Denmark) เมื่อคุณใช้ Scratcher
จัดทำขึ้นเพื่อให้เป็นไปตามข้อกำหนดของมาตรา 28 แห่ง GDPR

ข้อตกลงการประมวลผลข้อมูล

ข้อตกลงการประมวลผลข้อมูลฉบับนี้เป็นส่วนหนึ่งอันแยกไม่ได้ของข้อตกลงระหว่างลูกค้ากับ Scratcher
หากแนบข้อตกลงการประมวลผลข้อมูลฉบับนี้ไว้กับข้อตกลงหลัก ข้อ 10 ของข้อกำหนดและเงื่อนไขจะไม่มีผลบังคับใช้
และให้ใช้ข้อตกลงการประมวลผลข้อมูลฉบับนี้แทน

1. คำจำกัดความ

1.1. เว้นแต่บริบทจะกำหนดไว้เป็นอย่างอื่นอย่างชัดแจ้ง
คำที่ขึ้นต้นด้วยอักษรตัวใหญ่ต่อไปนี้ในข้อตกลงการประมวลผลข้อมูลฉบับนี้มีความหมายดังนี้

- “การละเมิดข้อมูล” คือการละเมิดความปลอดภัยของข้อมูลส่วนบุคคลโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย
  อันส่งผลให้ข้อมูลส่วนบุคคลที่ประมวลผลถูกทำลาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
  ไม่ว่าจะโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย
- “ผู้ควบคุมข้อมูล” หมายถึงลูกค้า เมื่อลูกค้าเป็นผู้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลตามที่นิยามไว้ใน GDPR
- “ผู้ประมวลผลข้อมูล” หมายถึง Scratcher เมื่อประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล
- “ข้อมูลส่วนบุคคล” หมายถึงข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวหรือสามารถระบุตัวได้ (มาตรา 4(1) แห่ง GDPR)
  ซึ่งผู้ประมวลผลข้อมูลประมวลผลในนามของผู้ควบคุมข้อมูลภายใต้ข้อตกลง
- “GDPR” หมายถึงกฎระเบียบ (EU) 2016/679 ของรัฐสภายุโรปและคณะมนตรีแห่งสหภาพยุโรป ลงวันที่ 27 เมษายน 2016
  ว่าด้วยการคุ้มครองบุคคลธรรมดาในส่วนที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการเคลื่อนย้ายข้อมูลดังกล่าวโดยเสรี
  และยกเลิกคำสั่ง 95/46/EC (กฎระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูล)
- “ผู้ประมวลผลช่วง” หมายถึงบุคคลใดๆ
  ที่ผู้ประมวลผลข้อมูลว่าจ้างให้ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ประมวลผลข้อมูลและตามคำสั่งของผู้ประมวลผลข้อมูล
  ภายในขอบเขตและเพื่อวัตถุประสงค์ที่ระบุไว้ในข้อตกลงการประมวลผลข้อมูล ทั้งนี้ไม่รวมพนักงานของผู้ประมวลผลข้อมูล

1.2. คำที่ขึ้นต้นด้วยอักษรตัวใหญ่ซึ่งไม่ได้นิยามไว้ข้างต้นมีความหมายตามที่นิยามไว้ในข้อตกลง
เว้นแต่บริบทจะกำหนดไว้เป็นอย่างอื่นอย่างชัดแจ้ง

2. ขอบเขต

2.1.
ข้อกำหนดและเงื่อนไขในข้อตกลงการประมวลผลข้อมูลฉบับนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้ประมวลผลข้อมูลในนามของและตามคำสั่งของผู้ควบคุมข้อมูล

2.2. ในกรณีที่ข้อตกลงการประมวลผลข้อมูลฉบับนี้กล่าวถึงผู้ประมวลผลข้อมูล
บทบัญญัติที่เกี่ยวข้องของข้อตกลงการประมวลผลข้อมูลให้ใช้บังคับกับผู้ประมวลผลช่วงที่ผู้ประมวลผลข้อมูลว่าจ้างด้วย

3. คำสั่งของผู้ควบคุมข้อมูลและเงื่อนไขการประมวลผล

3.1. ผู้ประมวลผลข้อมูลจะประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่เป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลเท่านั้น
รวมถึงในส่วนที่เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม
เว้นแต่กฎหมายของสหภาพหรือของรัฐสมาชิกที่ผู้ประมวลผลข้อมูลอยู่ภายใต้บังคับกำหนดให้ต้องดำเนินการเช่นนั้น ในกรณีดังกล่าว
ผู้ประมวลผลข้อมูลจะแจ้งข้อกำหนดทางกฎหมายนั้นให้ผู้ควบคุมข้อมูลทราบก่อนการประมวลผล
เว้นแต่กฎหมายนั้นห้ามการแจ้งข้อมูลดังกล่าวด้วยเหตุผลสำคัญด้านประโยชน์สาธารณะ

3.2. ผู้ประมวลผลข้อมูลจะประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลในประเภทที่ผู้ควบคุมข้อมูล (รวมถึงลูกค้าของผู้ควบคุมข้อมูล)
อัปโหลดหรือส่งเข้ามาเมื่อใช้บริการ
ประเภทของข้อมูลส่วนบุคคลและประเภทของเจ้าของข้อมูลที่ประมวลผลในนามของผู้ควบคุมข้อมูลระบุไว้ในภาคผนวก A
ของข้อตกลงการประมวลผลข้อมูลฉบับนี้

3.3.
คู่สัญญาตกลงให้ถือว่าข้อตกลงการประมวลผลข้อมูลฉบับนี้และข้อตกลงที่ผู้ควบคุมข้อมูลอาจทำขึ้นเมื่อใช้บริการเป็นคำสั่งที่เป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูล
ผู้ควบคุมข้อมูลอาจให้คำสั่งเพิ่มเติมที่เป็นลายลักษณ์อักษรแก่ผู้ประมวลผลข้อมูลเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลโดยปรับการตั้งค่าของบริการ คู่สัญญายังอาจตกลงกันเป็นลายลักษณ์อักษรเกี่ยวกับการปฏิบัติตามคำสั่งเพิ่มเติมของผู้ควบคุมข้อมูลและราคาของคำสั่งนั้นได้

3.4. ผู้ประมวลผลข้อมูลจะประมวลผลข้อมูลส่วนบุคคลตั้งแต่เวลาที่ผู้ควบคุมข้อมูลอัปโหลดหรือส่งข้อมูลเมื่อใช้บริการ จนกว่าข้อมูลจะถูกลบ
แต่ไม่เกินระยะเวลาที่กำหนดไว้ในข้อ 12 ของข้อตกลงการประมวลผลข้อมูลฉบับนี้

3.5. ผู้ประมวลผลข้อมูลจะแจ้งให้ผู้ควบคุมข้อมูลทราบโดยทันที หากเห็นว่าคำสั่งใดฝ่าฝืน GDPR
หรือบทบัญญัติอื่นของสหภาพหรือของรัฐสมาชิกว่าด้วยการคุ้มครองข้อมูล

3.6. ผู้ควบคุมข้อมูลตกลงว่า เมื่อผู้ประมวลผลข้อมูลร้องขอ จะจัดหาข้อมูล เอกสาร หรือความช่วยเหลือที่จำเป็นให้โดยไม่ชักช้า เพื่อให้ผู้ประมวลผลข้อมูลปฏิบัติตามข้อกำหนดทั้งหมดของ GDPR ได้อย่างถูกต้องเมื่อประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

4. การรักษาความลับของข้อมูลส่วนบุคคล

4.1. ผู้ประมวลผลข้อมูลจะใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการให้บริการและการใช้สิทธิของตนภายใต้ข้อตกลงเท่านั้น เว้นแต่กฎหมายกำหนดไว้เป็นอย่างอื่น ผู้ประมวลผลข้อมูลจะไม่เปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม

4.2.
ผู้ประมวลผลข้อมูลจะดูแลให้การเข้าถึงข้อมูลส่วนบุคคลจำกัดเฉพาะพนักงานหรือผู้ให้บริการของผู้ประมวลผลข้อมูลที่ต้องใช้ข้อมูลดังกล่าวเพื่อปฏิบัติหน้าที่หรือเพื่อให้บริการแก่ผู้ประมวลผลข้อมูล
และดูแลให้บุคคลทุกคนที่ได้รับอนุญาตให้ประมวลผลข้อมูลส่วนบุคคลผูกพันตนเองต่อการรักษาความลับ
หรืออยู่ภายใต้หน้าที่รักษาความลับตามกฎหมายที่เหมาะสม

4.3. หากผู้ประมวลผลข้อมูลมีหน้าที่ต้องเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่สาม (เช่น หน่วยงานบังคับใช้กฎหมาย) เพื่อปฏิบัติตามข้อกำหนดของกฎหมาย ผู้ประมวลผลข้อมูลจะแจ้งให้ผู้ควบคุมข้อมูลทราบทันทีถึงข้อกำหนดให้เปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่กฎหมายกำหนดไว้เป็นอย่างอื่น

4.4. หน้าที่รักษาความลับเหล่านี้ยังคงมีผลต่อไปหลังจากข้อตกลงการประมวลผลข้อมูลฉบับนี้สิ้นสุดลง

5. มาตรการทางเทคนิคและมาตรการเชิงองค์กร

5.1. โดยคำนึงถึงเทคโนโลยีที่ล้ำสมัย ต้นทุนการดำเนินการ ตลอดจนลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล รวมถึงความเสี่ยงที่มีโอกาสเกิดและความรุนแรงแตกต่างกันต่อสิทธิและเสรีภาพของบุคคลธรรมดา
ผู้ประมวลผลข้อมูลจะดำเนินมาตรการทางเทคนิคและมาตรการเชิงองค์กรที่เหมาะสมซึ่งจำเป็นเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล ก่อนการประมวลผลข้อมูลส่วนบุคคลและตลอดเวลาที่ประมวลผลข้อมูลส่วนบุคคล
ในการเลือกและดำเนินมาตรการทางเทคนิคและมาตรการเชิงองค์กรเพื่อให้มีระดับความปลอดภัยที่เพียงพอ
ผู้ประมวลผลข้อมูลจะพิจารณาเป็นพิเศษถึงความเสี่ยงที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล จากการทำลาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงโดยไม่ชอบด้วยกฎหมาย ต่อข้อมูลที่ส่ง จัดเก็บ หรือประมวลผลในลักษณะอื่น ไม่ว่าจะโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย

5.2. เนื่องจากผู้ประมวลผลข้อมูลเป็นผู้เชี่ยวชาญในสาขาของตนและมีความรู้และประสบการณ์ในการให้บริการ
ผู้ประมวลผลข้อมูลจะเลือกและกำหนดมาตรการทางเทคนิคและมาตรการเชิงองค์กรที่จำเป็นเพื่อบรรลุวัตถุประสงค์ตามข้อ 5.1 ของข้อตกลงการประมวลผลข้อมูลฉบับนี้ แต่มาตรการดังกล่าวต้องเป็นไปตามข้อกำหนดของกฎหมายที่ใช้บังคับในทุกกรณี อย่างไรก็ตาม
ผู้ควบคุมข้อมูลมีสิทธิให้คำสั่งและข้อเสนอแนะแก่ผู้ประมวลผลข้อมูลเกี่ยวกับการใช้มาตรการรักษาความปลอดภัยทางเทคนิคและเชิงองค์กร
ผู้ประมวลผลข้อมูลจะพิจารณาข้อเสนอแนะดังกล่าวของผู้ควบคุมข้อมูล และ (i)
ชี้แจงเหตุผลแก่ผู้ควบคุมข้อมูลว่าผู้ประมวลผลข้อมูลจะดำเนินการตามคำสั่งของผู้ควบคุมข้อมูลอย่างไร (ii)

ดำเนินการทันทีเพื่อนำมาตรการดังกล่าวไปปฏิบัติ

5.3. มาตรการทางเทคนิคและมาตรการเชิงองค์กรที่ผู้ประมวลผลข้อมูลดำเนินการ ณ เวลาที่ทำข้อตกลงการประมวลผลข้อมูลฉบับนี้ ได้อธิบายไว้ในภาคผนวก C ผู้ประมวลผลข้อมูลดูแลระบบการจัดการความปลอดภัยของข้อมูลที่ได้รับการรับรองตาม ISO/IEC 27001 และอาจปรับปรุงมาตรการเมื่อเวลาผ่านไป โดยต้องไม่ทำให้ระดับความปลอดภัยโดยรวมลดลง

5.4. โดยคำนึงถึงลักษณะของการประมวลผลและข้อมูลที่ผู้ประมวลผลข้อมูลมีอยู่
ผู้ประมวลผลข้อมูลจะช่วยเหลือผู้ควบคุมข้อมูลในการดูแลให้เป็นไปตามหน้าที่ตามมาตรา 32 แห่ง GDPR

6. การตรวจสอบการประมวลผลข้อมูล

6.1. ผู้ประมวลผลข้อมูลจะจัดให้ผู้ควบคุมข้อมูลเข้าถึงข้อมูลทั้งหมดที่จำเป็นเพื่อแสดงว่าเป็นไปตามหน้าที่ที่กำหนดไว้ในมาตรา 28 แห่ง GDPR รวมถึงใบรับรอง ISO/IEC 27001 ฉบับปัจจุบัน และเมื่อมีการร้องขอ ให้จัดหาเอกสารแสดงการนำมาตรการไปใช้ (Statement of Applicability) ด้วย

6.2. เพื่อตรวจสอบว่าผู้ประมวลผลข้อมูลประมวลผลข้อมูลส่วนบุคคลอย่างถูกต้องหรือไม่
ผู้ควบคุมข้อมูลมีสิทธิตรวจสอบการประมวลผลดังกล่าวภายใต้เงื่อนไขต่อไปนี้ (i)
การตรวจสอบต้องเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเท่านั้น (ii)
ผู้ควบคุมข้อมูลต้องแจ้งความประสงค์ที่จะตรวจสอบให้ผู้ประมวลผลข้อมูลทราบภายในระยะเวลาที่เหมาะสม ซึ่งต้องไม่น้อยกว่า 4 สัปดาห์ (iii)
ต้องดำเนินการตรวจสอบในลักษณะที่ไม่รบกวนการดำเนินงานประจำวันของผู้ประมวลผลข้อมูล (iv)
การตรวจสอบต้องดำเนินการโดยผู้ควบคุมข้อมูลเป็นผู้รับผิดชอบค่าใช้จ่าย (v)
การตรวจสอบต้องดำเนินการโดยบุคคลอิสระซึ่งต้องได้รับความเห็นชอบจากผู้ประมวลผลข้อมูลล่วงหน้า
โดยผู้ประมวลผลข้อมูลจะไม่ปฏิเสธการให้ความเห็นชอบโดยไม่มีเหตุอันสมควร
และบุคคลดังกล่าวต้องตกลงว่าจะปกป้องข้อมูลที่เป็นความลับของผู้ประมวลผลข้อมูล

6.3. ผู้ประมวลผลข้อมูลมีสิทธิได้รับค่าตอบแทนสำหรับความช่วยเหลือในการดำเนินการตรวจสอบ
จำนวนค่าตอบแทนดังกล่าวให้ผู้ประมวลผลข้อมูลเป็นผู้กำหนดโดยคำนึงถึงต้นทุนที่ผู้ประมวลผลข้อมูลต้องเสียไปในการตรวจสอบ
ผู้ประมวลผลข้อมูลจะแจ้งจำนวนค่าตอบแทนให้ผู้ควบคุมข้อมูลทราบก่อนการตรวจสอบ

6.4. การตรวจสอบและการตรวจตราที่หน่วยงานกำกับดูแลที่มีอำนาจดำเนินการไม่อยู่ภายใต้เงื่อนไขในข้อ 6.2 และ 6.3

6.5. หากผู้ควบคุมข้อมูลไม่พอใจผลการตรวจสอบ
ผู้ควบคุมข้อมูลมีสิทธิบอกเลิกข้อตกลงการประมวลผลข้อมูลฉบับนี้และข้อตกลงฝ่ายเดียวโดยไม่ต้องผ่านกระบวนการทางศาล ในกรณีนี้ การบอกเลิกข้อตกลงทั้งสองฉบับเป็นมาตรการเดียวที่ผู้ควบคุมข้อมูลอาจดำเนินการได้ และผู้ประมวลผลข้อมูลไม่มีหน้าที่ชดเชยความเสียหายใดๆ แก่ผู้ควบคุมข้อมูล

7. ผู้ประมวลผลช่วง

7.1.

ผู้ควบคุมข้อมูลขอให้ความยินยอมทั่วไปล่วงหน้าแก่ผู้ประมวลผลข้อมูลในการว่าจ้างผู้ประมวลผลช่วงที่จะประมวลผลข้อมูลส่วนบุคคลในนามของผู้ประมวลผลข้อมูล ภายในขอบเขตและเพื่อวัตถุประสงค์ที่ระบุไว้ในข้อตกลงการประมวลผลข้อมูลฉบับนี้

7.2. ผู้ประมวลผลข้อมูลจะดูแลให้มีข้อตกลงเป็นลายลักษณ์อักษรกับผู้ประมวลผลช่วงที่ว่าจ้าง
โดยผู้ประมวลผลช่วงตกลงปฏิบัติตามหน้าที่คุ้มครองข้อมูลเช่นเดียวกับที่กำหนดไว้ในข้อตกลงการประมวลผลข้อมูลฉบับนี้
โดยเฉพาะการให้หลักประกันที่เพียงพอในการดำเนินมาตรการทางเทคนิคและมาตรการเชิงองค์กรที่เหมาะสม
เพื่อให้การประมวลผลเป็นไปตามข้อกำหนดของ GDPR
ผู้ประมวลผลข้อมูลต้องรับผิดต่อผู้ควบคุมข้อมูลในการปฏิบัติตามหน้าที่ของผู้ประมวลผลช่วง

7.3. รายชื่อผู้ประมวลผลช่วงปัจจุบันระบุไว้ในภาคผนวก B ของข้อตกลงการประมวลผลข้อมูลฉบับนี้
ผู้ประมวลผลข้อมูลจะแจ้งให้ผู้ควบคุมข้อมูลทราบถึงแผนการเปลี่ยนหรือว่าจ้างผู้ประมวลผลช่วงรายใหม่
โดยเปิดเผยข้อมูลดังกล่าวให้ผู้ควบคุมข้อมูลทราบไม่น้อยกว่า 14 วันตามปฏิทินก่อนเหตุการณ์ที่วางแผนไว้

7.4. หากผู้ควบคุมข้อมูลยังคงใช้บริการต่อไปหลังจากมีการเปลี่ยนหรือว่าจ้างผู้ประมวลผลช่วงรายใหม่
ภายหลังได้รับแจ้งจากผู้ประมวลผลข้อมูลตามขั้นตอนที่กำหนดในข้อ 7.3 ของข้อตกลงการประมวลผลข้อมูลฉบับนี้
ให้ถือว่าผู้ควบคุมข้อมูลยินยอมต่อการดำเนินการดังกล่าวของผู้ประมวลผลข้อมูล
หากผู้ควบคุมข้อมูลไม่เห็นด้วยกับการเปลี่ยนหรือการว่าจ้างผู้ประมวลผลช่วงดังกล่าว
ผู้ควบคุมข้อมูลมีสิทธิบอกเลิกข้อตกลงฝ่ายเดียวโดยไม่ต้องผ่านกระบวนการทางศาล ในกรณีเช่นนี้
การบอกเลิกข้อตกลงเป็นมาตรการเดียวที่ผู้ควบคุมข้อมูลอาจดำเนินการได้ และผู้ประมวลผลข้อมูลไม่มีหน้าที่ชดเชยความเสียหายใดๆ
แก่ผู้ควบคุมข้อมูล

7.5. หากผู้ควบคุมข้อมูลถอนความยินยอมทั่วไปในการว่าจ้างผู้ประมวลผลช่วง
ผู้ประมวลผลข้อมูลมีสิทธิบอกเลิกข้อตกลงฝ่ายเดียวโดยไม่ต้องผ่านกระบวนการทางศาล และให้ถือว่าการบอกเลิกดังกล่าวเกิดจากเหตุผลสำคัญ
และให้ถือว่าผู้ควบคุมข้อมูลไม่ได้รับความเสียหายใดๆ จากการบอกเลิกนั้น

8. การละเมิดข้อมูล

8.1. ผู้ประมวลผลข้อมูลจะแจ้งให้ผู้ควบคุมข้อมูลทราบถึงการละเมิดข้อมูลใดๆ ที่กระทบต่อข้อมูลส่วนบุคคล
ผ่านที่อยู่อีเมลที่ระบุในข้อเสนอการขาย หรือหากไม่ได้ระบุไว้ ให้แจ้งทางที่อยู่อีเมลของเจ้าของบัญชีของผู้ควบคุมข้อมูล
โดยไม่ชักช้าเกินสมควรและไม่เกิน 24 ชั่วโมงนับแต่ทราบถึงการละเมิดข้อมูล และโดยคำนึงถึงลักษณะของบริการที่ให้
การประมวลผลข้อมูลส่วนบุคคล และข้อมูลที่มีอยู่ จะให้ข้อมูลต่อไปนี้แก่ผู้ควบคุมข้อมูล (i) ลักษณะของการละเมิดข้อมูล
รวมถึงประเภทของเจ้าของข้อมูลและจำนวนโดยประมาณ หากสามารถระบุได้ (ii) ผลที่อาจเกิดขึ้นจากการละเมิดข้อมูล (iii)
มาตรการที่ผู้ประมวลผลข้อมูลได้ดำเนินการหรือเสนอให้ดำเนินการเพื่อจัดการกับการละเมิดข้อมูล
รวมถึงมาตรการบรรเทาผลกระทบด้านลบที่อาจเกิดขึ้นจากการละเมิดข้อมูล หากเหมาะสม (iv)

ชื่อเต็มและข้อมูลติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลหรือบุคคลอื่นที่สามารถให้ข้อมูลเพิ่มเติมได้

8.2. ผู้ประมวลผลข้อมูลจะบันทึกการละเมิดข้อมูลทั้งหมด รวมถึงข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูล ผลกระทบ และมาตรการแก้ไขที่ดำเนินการ ในกรณีที่ GDPR หรือกฎหมายอื่นที่ใช้บังคับกำหนดไว้ ผู้ประมวลผลข้อมูลจะส่งเอกสารบันทึกดังกล่าวให้หน่วยงานกำกับดูแล

8.3. โดยคำนึงถึงลักษณะของการประมวลผลและข้อมูลที่ผู้ประมวลผลข้อมูลมีอยู่
ผู้ประมวลผลข้อมูลจะช่วยเหลือผู้ควบคุมข้อมูลในการดูแลให้เป็นไปตามหน้าที่ตามมาตรา 33 และ 34 แห่ง GDPR
ผู้ควบคุมข้อมูลยังคงมีหน้าที่รับผิดชอบในการแจ้งหน่วยงานกำกับดูแลและแจ้งเจ้าของข้อมูลเมื่อมีความจำเป็น
ยกเว้นกรณีที่การละเมิดข้อมูลเกิดจากการที่ผู้ประมวลผลข้อมูลฝ่าฝืนหน้าที่ตามข้อตกลงการประมวลผลข้อมูลฉบับนี้
ความช่วยเหลือของผู้ประมวลผลข้อมูลนอกเหนือจากการแจ้งเตือนตามข้อ 8.1 อาจมีค่าใช้จ่ายเพิ่มเติม

9. การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม

9.1. การโอนข้อมูลส่วนบุคคลใดๆ ไปยังประเทศที่สาม (นอก EU/EEA)
โดยผู้ประมวลผลข้อมูลจะกระทำได้ก็ต่อเมื่ออาศัยคำสั่งที่เป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลเท่านั้น และต้องเป็นไปตามบทที่ V ของ GDPR เสมอ

9.2. การที่ผู้ควบคุมข้อมูลอนุมัติผู้ประมวลผลช่วงที่ระบุไว้ในภาคผนวก B
ถือเป็นคำสั่งที่เป็นลายลักษณ์อักษรสำหรับการโอนข้อมูลที่ผู้ประมวลผลช่วงเหล่านั้นดำเนินการตามที่อธิบายไว้ในภาคผนวกดังกล่าว
การโอนข้อมูลแต่ละครั้งต้องอาศัยการตัดสินว่ามีระดับการคุ้มครองที่เพียงพอของคณะกรรมาธิการยุโรป
(รวมถึงกรอบความเป็นส่วนตัวของข้อมูล EU–US สำหรับผู้รับที่ได้รับการรับรอง) ข้อสัญญามาตรฐานของคณะกรรมาธิการยุโรป
หรือกลไกการโอนข้อมูลอื่นภายใต้บทที่ V ของ GDPR

10. ความร่วมมือ

10.1. โดยคำนึงถึงลักษณะของบริการที่ให้และการประมวลผลข้อมูลลูกค้า รวมถึงข้อมูลที่มีอยู่
ผู้ประมวลผลข้อมูลจะให้ความร่วมมือกับผู้ควบคุมข้อมูลเพื่อให้การปฏิบัติตามหน้าที่ที่ระบุไว้ในมาตรา 32–36 แห่ง GDPR เป็นไปอย่างถูกต้อง
เพื่อวัตถุประสงค์นี้ และเฉพาะภายในขอบเขตที่ระบุไว้ในข้อตกลงการประมวลผลข้อมูลฉบับนี้
ผู้ประมวลผลข้อมูลจะให้ข้อมูลที่ร้องขอซึ่งจำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลตาม GDPR อย่างถูกต้องแก่ผู้ควบคุมข้อมูล

10.2. ในกรณีที่ประเภทของการประมวลผล โดยเฉพาะการใช้เทคโนโลยีใหม่ และเมื่อคำนึงถึงลักษณะ ขอบเขต บริบท
และวัตถุประสงค์ของการประมวลผล มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา
ผู้ประมวลผลข้อมูลจะสนับสนุนผู้ควบคุมข้อมูลในการประเมินผลกระทบของการประมวลผลที่คาดการณ์ไว้ต่อการคุ้มครองข้อมูลส่วนบุคคล
ก่อนการประมวลผล

10.3. หากเจ้าของข้อมูล หน่วยงานกำกับดูแล หรือบุคคลที่สามร้องขอให้ผู้ประมวลผลข้อมูลให้ข้อมูลใดๆ
เกี่ยวกับข้อมูลส่วนบุคคลที่ประมวลผลตามที่กฎหมายกำหนด
ผู้ประมวลผลข้อมูลจะส่งต่อคำร้องขอดังกล่าวให้ผู้ควบคุมข้อมูลโดยไม่ชักช้าเกินสมควร

ผู้ประมวลผลข้อมูลรับรองว่าจะช่วยเหลือผู้ควบคุมข้อมูลเท่าทีจำเป็นในการตอบคำร้องขอของเจ้าของข้อมูล หน่วยงานกำกับดูแล หรือบุคคลทีสาม และในการปฏิบัติตามหน้าทีของผู้ควบคุมข้อมูลทีเกียวกับการดำเนินการตามสิทธิของเจ้าของข้อมูล
ซึงรวมถึงแต่ไม่จำกัดเพียงสิทธิในการแก้ไขและการลบข้อมูลส่วนบุคคล สิทธิในการโอนย้ายข้อมูลส่วนบุคคล
สิทธิในการคัดค้านและการจำกัดการประมวลผล
ผู้ประมวลผลข้อมูลจะดูแลให้ข้อมูลทีอยู่ในความครอบครองถูกส่งมอบภายในกรอบเวลาทีกฎหมายกำหนด

11. หน้าทีของผู้ควบคุมข้อมูล

11.1.
ผู้ควบคุมข้อมูลเป็นผู้กำหนดประเภทของข้อมูลส่วนบุคคลและประเภทของเจ้าของข้อมูลทีจะมอบให้ผู้ประมวลผลข้อมูลตามดุลยพินิจและความรับผิดชอบของตนแต่เพียงผู้เดียว และจะมอบเฉพาะข้อมูลส่วนบุคคลทีจำเป็นต่อการให้บริการอย่างถูกต้องของผู้ประมวลผลข้อมูลเท่านัน
ผู้ควบคุมข้อมูลเป็นผู้รับความเสียงทังหมดทีเกียวข้อง รวมถึงความเสียงทีผู้ประมวลผลข้อมูลจะได้รับข้อมูลส่วนบุคคลมากกว่าทีจำเป็น

11.2.
ผู้ควบคุมข้อมูลรับรองและยืนยันว่าได้รับและจะรักษาไว้ตลอดอายุของข้อตกลงซึงใบอนุญาตและการอนุมัติทังหมดทีจำเป็นในการมอบข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลและในการว่าจ้างผู้ประมวลผลข้อมูลให้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลง

12. การลบและการส่งคืนข้อมูลส่วนบุคคล

12.1. เมือข้อตกลงหรือข้อตกลงการประมวลผลข้อมูลฉบับนีสินสุดลง ผู้ประมวลผลข้อมูลจะต้องดำเนินการตามทีผู้ควบคุมข้อมูลเลือก โดยลบข้อมูลส่วนบุคคลทังหมดทีประมวลผลในนามของผู้ควบคุมข้อมูล หรือส่งคืนข้อมูลส่วนบุคคลทังหมดให้ผู้ควบคุมข้อมูล (ผู้ควบคุมข้อมูลสามารถส่งออกข้อมูลของตนจากบริการได้ตลอดเวลา) และลบสำเนาทีมีอยู่ทังหมด
พร้อมรับรองต่อผู้ควบคุมข้อมูลว่าได้ดำเนินการแล้ว เว้นแต่กฎหมายของสหภาพหรือของรัฐสมาชิกกำหนดให้ต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ สำเนาในข้อมูลสำรองจะถูกลบเมือข้อมูลสำรองหมดอายุตามรอบปกติ และจะไม่ถูกนำไปใช้เพือวัตถุประสงค์อืนใดในระหว่างนัน

13. ความรับผิด

13.1. ไม่ว่าผู้ควบคุมข้อมูลจะได้รับความเสียหายใดๆ
ความรับผิดทังหมดของผู้ประมวลผลข้อมูลภายใต้ข้อตกลงการประมวลผลข้อมูลฉบับนีจำกัดดังนี
ความรับผิดรวมของผู้ประมวลผลข้อมูลและผู้ให้บริการของผู้ประมวลผลข้อมูลสำหรับข้อเรียกร้องทังหมดทีเกิดขึนภายใต้หรือเกียวข้องกับข้อตกลงการประมวลผลข้อมูลฉบับนี จะต้องไม่เกินจำนวนเงินทีผู้ควบคุมข้อมูลชำระจริงให้ผู้ประมวลผลข้อมูลสำหรับบริการในช่วงสิบสอง (12) เดือนก่อนวันทีเกิดเหตุอันเป็นต้นเหตุของข้อเรียกร้อง ภายใต้ขอบเขตสูงสุดทีกฎหมายทีใช้บังคับอนุญาต
ไม่ว่ากรณีใดผู้ประมวลผลข้อมูลหรือผู้ให้บริการของผู้ประมวลผลข้อมูลจะไม่ต้องรับผิดต่อความเสียหายพิเศษ ความเสียหายทีเกิดขึนโดยบังเอิญ ความเสียหายทางอ้อม หรือความเสียหายสืบเนืองใดๆ (รวมถึงแต่ไม่จำกัดเพียงความเสียหายจากการสูญเสียกำไร ข้อมูล หรือสารสนเทศอืน การหยุดชะงักของธุรกิจ การบาดเจ็บส่วนบุคคล การสูญเสียความเป็นส่วนตัว)
แม้ผู้ประมวลผลข้อมูลหรือผู้ให้บริการจะได้รับแจ้งถึงความเป็นไปได้ของความเสียหายดังกล่าว

และแม้วิธีการเยียวยาจะไม่บรรลุวัตถุประสงค์สำคัญก็ตาม

13.2. ข้อจำกัดในข้อ 13.1 ใช้บังคับระหว่างคู่สัญญาเท่านั้น ไม่ใช้บังคับกับความรับผิดที่ไม่อาจจำกัดได้ตามกฎหมายที่ใช้บังคับ และไม่กระทบต่อสิทธิของเจ้าของข้อมูลตามมาตรา 82 แห่ง GDPR

14. ผลใช้บังคับและการสิ้นสุด

14.1. ข้อตกลงการประมวลผลข้อมูลฉบับนี้มีผลใช้บังคับเมื่อข้อตกลงมีผลใช้บังคับ และคงมีผลต่อไปตราบเท่าที่ข้อตกลงยังมีผลใช้บังคับ หน้าที่ของผู้ประมวลผลข้อมูลยังคงอยู่ตราบเท่าที่ผู้ประมวลผลข้อมูลยังประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

15. บทบัญญัติสุดท้าย

15.1. ผู้ประมวลผลข้อมูลจะแจ้งการเปลี่ยนแปลงข้อตกลงการประมวลผลข้อมูลที่ตั้งใจจะทำล่วงหน้าอย่างน้อย 30 วันก่อนการเปลี่ยนแปลงนั้น หากผู้ควบคุมข้อมูลยังคงใช้บริการต่อไปหลังจากมีการประกาศการเปลี่ยนแปลงข้อตกลงการประมวลผลข้อมูล ให้ถือว่าผู้ควบคุมข้อมูลเห็นชอบกับการเปลี่ยนแปลงข้อตกลงการประมวลผลข้อมูล หากผู้ควบคุมข้อมูลไม่เห็นด้วยกับการเปลี่ยนแปลง ผู้ควบคุมข้อมูลจะไม่สามารถใช้บริการได้และมีสิทธิบอกเลิกข้อตกลง

15.2. ในกรณีที่ข้อตกลงการประมวลผลข้อมูลฉบับนี้ขัดแย้งกับข้อตกลง ให้ข้อตกลงการประมวลผลข้อมูลฉบับนี้มีผลเหนือกว่าในส่วนที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

15.3. ข้อตกลงการประมวลผลข้อมูลฉบับนี้อยู่ภายใต้กฎหมายเดียวกัน และการระงับข้อพิพาทให้ดำเนินการในลักษณะเดียวกันตามที่กำหนดไว้ในข้อตกลง

15.4. ภาคผนวก

- ภาคผนวก A: รายละเอียดการประมวลผลข้อมูลส่วนบุคคล
- ภาคผนวก B: ผู้ประมวลผลช่วงที่ได้รับอนุมัติ
- ภาคผนวก C: มาตรการทางเทคนิคและมาตรการเชิงองค์กร

ภาคผนวก A – รายละเอียดการประมวลผลข้อมูลส่วนบุคคล

เรื่องที่ประมวลผลและระยะเวลา	การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบริการตลอดอายุของข้อตกลง และหลังจากนั้นจนกว่าข้อมูลส่วนบุคคลจะถูกลบหรือส่งคืนตามข้อ 12

ลักษณะของการประมวลผล	การโฮสต์และจัดเก็บข้อมูล การเก็บรวบรวมข้อมูลส่วนบุคคลผ่านแคมเปญและฟอร์มของผู้ควบคุมข้อมูล การแสดงผล ส่งออก และลบข้อมูลในบริการ การส่งอีเมลและข้อความถึงผู้เข้าร่วมตามที่ผู้ควบคุมข้อมูลตั้งค่าไว้ (เช่น การยืนยัน รหัส และการแจ้งรางวัล) การส่งต่อข้อมูลไปยังระบบของผู้ควบคุมข้อมูลเองผ่านการเชื่อมต่อ Webhook และ API ตามคำสั่งของผู้ควบคุมข้อมูล การสนับสนุนและการจัดการข้อผิดพลาด
วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล	เพื่อให้ผู้ควบคุมข้อมูลใช้บริการของผู้ประมวลผลข้อมูลได้ตามที่ตกลงกันในข้อตกลง
การดำเนินการประมวลผลข้อมูลส่วนบุคคล	การเก็บรวบรวมและจัดเก็บข้อมูลลูกค้า รวมถึงข้อมูลส่วนบุคคลที่ให้ไว้ระหว่างการใช้บริการ
ประเภทของข้อมูลส่วนบุคคล	ชื่อ นามสกุล อีเมล ที่อยู่ IP และตำแหน่งโดยประมาณที่ได้จากที่อยู่ IP วันและเวลาที่ลงทะเบียน (created at) และข้อมูลเพิ่มเติม เช่น วันเกิดและหมายเลขโทรศัพท์ (หากลูกค้าเก็บรวบรวม) ทั้งนี้ ขึ้นอยู่กับวิธีที่ผู้ควบคุมข้อมูลตั้งค่าแคมเปญ อาจรวมถึงคำตอบของคำถามในแคมเปญ ผลการเล่นเกมและรางวัลที่ได้รับ รหัส บันทึกความยินยอม ไฟล์ที่ผู้เข้าร่วมอัปโหลด (เช่น รูปภาพ) และข้อมูลทางเทคนิค เช่น ข้อมูลเบราว์เซอร์และอุปกรณ์
ข้อมูลประเภทพิเศษ	ไม่มีเจตนาให้เก็บ ผู้ควบคุมข้อมูลต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลประเภทพิเศษ (มาตรา 9 แห่ง GDPR) หรือข้อมูลเกี่ยวกับการต้องโทษทางอาญา (มาตรา 10 แห่ง GDPR) ผ่านบริการ เว้นแต่ตกลงกันเป็นลายลักษณ์อักษร
ประเภทของเจ้าของข้อมูล	ผู้เข้าร่วมแคมเปญของผู้ควบคุมข้อมูล (ลูกค้า) ผู้เข้าชมแคมเปญของผู้ควบคุมข้อมูลที่ไม่ได้ลงทะเบียน (ที่อยู่ IP ตำแหน่งโดยประมาณ และข้อมูลเบราว์เซอร์) และผู้ใช้บริการของผู้ควบคุมข้อมูล เท่าที่ข้อมูลของบุคคลเหล่านี้ถูกประมวลผลในนามของผู้ควบคุมข้อมูล

สถานที่ประมวลผลข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะถูกประมวลผลในสถานที่ของผู้ประมวลผลข้อมูลและบนเซิร์ฟเวอร์เสมือนที่ตั้งอยู่ในสหภาพยุโรป และโดยผู้ประมวลผลช่วงที่ระบุไว้ในภาคผนวก B ณ สถานที่ที่ระบุไว้ในภาคผนวกดังกล่าว
ระยะเวลาการประมวลผล/ระยะเวลาการจัดเก็บ	ตามที่ผู้ควบคุมข้อมูลกำหนดในบริการ ทั้งนี้ ตามข้อ 9.4 ของข้อกำหนดและเงื่อนไข ผู้ประมวลผลข้อมูลอาจลบข้อมูลส่วนบุคคลที่เก่ากว่าสาม (3) ปี

ภาคผนวก B – ผู้ประมวลผลช่วงที่ได้รับอนุมัติ

ณ เวลาที่ทำข้อตกลงการประมวลผลข้อมูล ผู้ควบคุมข้อมูลอนุมัติการว่าจ้างผู้ประมวลผลช่วงที่ระบุไว้ด้านล่าง การโอนข้อมูลออกนอก EU/EEA อาศัยกรอบความเป็นส่วนตัวของข้อมูล EU–US เมื่อผู้รับได้รับการรับรอง หรืออาศัยข้อสัญญามาตรฐานของคณะกรรมาธิการยุโรป (ข้อ 9.2)

ผู้ประมวลผลช่วง	คำอธิบายการประมวลผล	สถานที่ประมวลผล
Amazon Web Services EMEA SARL, Luxembourg (AWS)	การโฮสต์บริการ ได้แก่ เซิร์ฟเวอร์ ฐานข้อมูล พื้นที่จัดเก็บไฟล์ ข้อมูลสำรอง แคช และบันทึกระบบ	สหภาพยุโรป (สตอกโฮล์ม สวีเดน) เนื้อหาถูกส่งผ่านเครือข่าย Amazon CloudFront ซึ่งอาจประมวลผลทราฟฟิกที่จุดให้บริการ (edge) นอก EU/EEA
ClickHouse, Inc. (ClickHouse Cloud)	ฐานข้อมูลวิเคราะห์ข้อมูลสำหรับสถิติแคมเปญ เช่น การเข้าชม การร่วมสนุก และการลงทะเบียน รวมถึงที่อยู่ IP และข้อมูลเบราว์เซอร์	สหภาพยุโรป (แฟรงก์เฟิร์ต เยอรมนี) โฮสต์บน AWS
Mailgun Technologies, Inc. (part of Sinch)	การส่งอีเมลที่ผู้ควบคุมข้อมูลตั้งค่าไว้ถึงผู้เข้าร่วม เช่น การยืนยัน รหัส และการแจ้งรางวัล รวมถึงการส่งถึง การเปิดอ่าน และการคลิก เมื่อเปิดใช้การติดตามผล	สหภาพยุโรป (ภูมิภาค EU สำหรับข้อมูลข้อความ) ข้อมูลบัญชีจำนวนจำกัดอาจถูกประมวลผลทั่วโลก
ip-api.com	การค้นหาตำแหน่งโดยประมาณจากที่อยู่ IP ของผู้เข้าร่วม และการตรวจจับทราฟฟิกจากพร็อกซีและดาต้าเซ็นเตอร์ เพื่อป้องกันการฉ้อโกงและบอต	โรมาเนีย (EU) ไม่อาจตัดความเป็นไปได้ที่จะมีการประมวลผลหรือโอนข้อมูลนอก EU/EEA

ผู้ประมวลผลช่วง	คำอธิบายการประมวลผล	สถานที่ประมวลผล
Google (Gemini API)	ฟีเจอร์ AI ในบริการ เช่น ผู้ช่วย AI การแปล และการสร้างข้อความ ข้อมูลผู้เข้าร่วมจะถูกส่งในรูปแบบที่ใช้นามแฝงหรือรวมกลุ่มเท่านั้น (เช่น อักษรย่อ โดเมนอีเมล และเวลาที่ลงทะเบียน) เว้นแต่ผู้ใช้ของผู้ควบคุมข้อมูลจะป้อนข้อมูลดังกล่าวเอง	สหรัฐอเมริกา และอาจรวมถึงประเทศอื่น ขึ้นอยู่กับปลายทาง API และการตั้งค่าการประมวลผล
Functional Software, Inc. (Sentry)	การตรวจสอบข้อผิดพลาดและการเล่นซ้ำเซสชันของบริการ เพื่อค้นหาและแก้ไขข้อผิดพลาด รายงานอาจมีรหัสผู้ใช้และรหัสบัญชีภายใน และข้อมูลทางเทคนิคเกี่ยวกับเบราว์เซอร์ของผู้ใช้ของผู้ควบคุมข้อมูล ข้อความในการเล่นซ้ำเซสชันจะถูกปิดบัง	สหภาพยุโรป (เยอรมนี ภูมิภาค Sentry EU)
Cloudflare, Inc. (Turnstile)	การป้องกันบอตบนฟอร์มของแคมเปญ เมื่อผู้ควบคุมข้อมูลเปิดใช้สำหรับแคมเปญนั้นเท่านั้น ได้รับที่อยู่ IP และสัญญาณจากเบราว์เซอร์ของผู้เข้าร่วม	เครือข่ายทั่วโลก การประมวลผลอาจเกิดขึ้นนอก EU/EEA
Features & Labels, Inc. (fal.ai)	การสร้างและแก้ไขภาพด้วย AI การลบพื้นหลัง และการพากย์เสียงในบริการ ได้รับพรอมต์และรูปภาพที่ผู้ใช้ของผู้ควบคุมข้อมูลส่งเข้ามา	สหรัฐอเมริกา
Adressevælger (adressevaelger.dk)	คำแนะนำที่อยู่ในฟอร์มของแคมเปญ เมื่อผู้ควบคุมข้อมูลเปิดใช้สำหรับแคมเปญนั้นเท่านั้น ได้รับข้อความที่อยู่ที่ผู้เข้าร่วมพิมพ์และที่อยู่ IP ของผู้เข้าร่วม	เดนมาร์ก (EU)

ภาคผนวก C – มาตรการทางเทคนิคและมาตรการเชิงองค์กร

ผู้ประมวลผลข้อมูลดูแลระบบการจัดการความปลอดภัยของข้อมูลที่ได้รับการรับรองตาม ISO/IEC 27001:2022 โดย Bureau Veritas (ใบรับรองเลขที่ FIHSK27150F) มาตรการประกอบด้วย

- **การโฮสต์และความปลอดภัยทางกายภาพ:** ข้อมูลลูกค้าทั้งหมดจัดเก็บในดาต้าเซ็นเตอร์ของ Amazon Web Services (AWS) ในสหภาพยุโรป ผู้ประมวลผลข้อมูลไม่ได้ดูแลเซิร์ฟเวอร์ของตนเอง ความปลอดภัยทางกายภาพและด้านสิ่งแวดล้อมจัดให้โดย AWS ซึ่งได้รับการรับรอง ISO 27001 และ SOC 2
- **ความปลอดภัยของเครือข่าย:** เซิร์ฟเวอร์และฐานข้อมูลทำงานในเครือข่ายส่วนตัว (Amazon VPC) ที่ไม่สามารถเข้าถึงได้จากอินเทอร์เน็ต มีเพียงตัวกระจายโหลดและเครือข่ายกระจายเนื้อหาเท่านั้นที่เปิดสู่สาธารณะ โดยได้รับการปกป้องด้วยไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (AWS WAF) และการป้องกัน DDoS
- **การเข้ารหัส:** ทราฟฟิกทั้งหมดเข้ารหัสด้วย TLS (HTTPS) ฐานข้อมูล ไฟล์ และข้อมูลสำรองเข้ารหัสขณะจัดเก็บด้วย AES-256 ข้อมูลรับรองสำหรับการเชื่อมต่อยังถูกเข้ารหัสเพิ่มเติมในระดับแอปพลิเคชัน รหัสผ่านถูกแฮชและเพิ่มเกลือด้วย bcrypt
- **การควบคุมการเข้าถึง:** การควบคุมการเข้าถึงตามบทบาทสำหรับผู้ใช้ของลูกค้า การยืนยันตัวตนสองขั้นตอนและ Google single sign-on การหมดเวลาของเซสชัน และการจำกัดอัตราการพยายามเข้าสู่ระบบ การเข้าถึงของพนักงานเป็นไปตามหลักสิทธิขั้นต่ำและหลักจำเป็นต้องรู้ ใช้บัญชีเฉพาะบุคคลและการยืนยันตัวตนหลายปัจจัยเท่าที่เป็นไปได้ ได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง และถูกเพิกถอนเมื่อมีผู้ลาออก
- **การแยกข้อมูล:** ข้อมูลลูกค้าถูกแยกเชิงตรรกะตามบัญชี (การแยกผู้เช่า) และทุกคำขอต้องผ่านการอนุญาต
- **การบันทึกและการเฝ้าติดตาม:** การเปลี่ยนแปลงโครงสร้างพื้นฐานถูกบันทึกในร่องรอยการตรวจสอบที่ป้องกันการแก้ไข บันทึกของแอปพลิเคชันถูกรวบรวมไว้ศูนย์กลาง แพลตฟอร์มถูกเฝ้าติดตามตลอด 24 ชั่วโมง และลูกค้าสามารถดูกิจกรรมของผู้ใช้ของตนได้ในบันทึกกิจกรรม
- **ความพร้อมใช้งานและความยืดหยุ่น:** ข้อมูลสำรองที่เข้ารหัสรายวัน เก็บไว้อย่างน้อยเจ็ดวันและจัดเก็บแยกจากระบบใช้งานจริง ทดสอบการกู้คืนอย่างน้อยปีละหนึ่งครั้ง และมีแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนจากภัยพิบัติที่ได้รับการทบทวนและซ้อมทุกปี
- **การจัดการเหตุการณ์:** กระบวนการที่จัดทำเป็นเอกสารสำหรับรายงาน ประเมิน ควบคุม วิเคราะห์ และติดตามผลเหตุการณ์ด้านความปลอดภัย รวมถึงการแจ้งการละเมิดข้อมูลตามข้อ 8
- **การพัฒนาและการดำเนินงานอย่างปลอดภัย:** เซิร์ฟเวอร์ทำงานเป็นคอนเทนเนอร์ที่เปลี่ยนแปลงไม่ได้ (immutable) โดยไม่มีการเข้าถึงผ่าน SSH และไม่เคยถูกแก้ไขด้วยมือ และการเปลี่ยนแปลงต้องผ่านการทดสอบก่อนปล่อยใช้งาน
- **บุคลากร:**
  พนักงานผูกพันตามหน้าที่รักษาความลับและได้รับการฝึกอบรมด้านความตระหนักรู้เรื่องความปลอดภัยของข้อมูลเป็นส่วนหนึ่งของระบบการจัดการความปลอดภัยของข้อมูล พาร์ตเนอร์ที่เข้าถึงโครงสร้างพื้นฐานได้ล้วนได้รับการรับรอง ISO 27001 ด้วยตนเอง และได้รับสิทธิการเข้าถึงเฉพาะเท่าที่งานของตนต้องการ
- **เครื่องมือลดข้อมูลให้น้อยที่สุดและลบข้อมูล:** ผู้ควบคุมข้อมูลเป็นผู้ตัดสินใจว่าแต่ละแคมเปญเก็บข้อมูลใดบ้าง และสามารถส่งออก ลบ หรือตั้งให้ลบข้อมูลผู้เข้าร่วมโดยอัตโนมัติได้