



สมาคมนายหน้าประกันภัยไทย
Thai Insurance Brokers Association

**แนวทางปฏิบัติของนายหน้าประกันภัยนิติบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**

สมาคมนายหน้าประกันภัยไทย

(วันที่ 1 พฤษภาคม พ.ศ. 2565)

คำนำ

เรื่อง แนวทางปฏิบัติของนายหน้าประกันภัยนิติบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
เรียน สมาชิกสมาคมนายหน้าประกันภัยไทย

ตามที่สมาชิกสมาคมนายหน้าประกันภัยไทยได้สอบถามและขอหารือ เกี่ยวกับประกาศกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งทางสมาคมนายหน้าประกันภัยไทย ได้มีการจัดสัมมนาส่งเสริมความรู้เกี่ยวกับประเด็นดังกล่าวในหลายครั้งที่ผ่านมา รวมถึงได้ส่งข้อมูลข่าวสารต่างๆอันเป็นประโยชน์ที่เกี่ยวข้องกับกฎหมายดังกล่าว เพื่อให้สมาชิกได้ศึกษาหาข้อมูลและพร้อมปฏิบัติเพื่อให้เป็นไปตามข้อกำหนดที่กำหนด

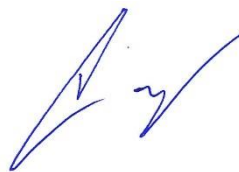
อย่างไรก็ตาม การใช้บังคับกฎหมายดังกล่าวจะเริ่มมีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ.2565 นี้ ซึ่งในขณะนี้บริษัทนายหน้าประกันภัยหลายรายยังไม่แน่ใจถึงแนวทางที่จะต้องนำไปปฏิบัติเพื่อให้เป็นไปตามกฎหมายดังกล่าวอย่างถูกต้องทางสมาคมนายหน้าประกันภัยไทย จึงนำเสนอข้อมูลอันจำเป็นเพื่อเป็นแนวทางในการปฏิบัติงานของนายหน้าประกันภัย มา ณ ที่นี้ อย่างไรก็ตามแนวทางปฏิบัติดังกล่าวจะขึ้นอยู่กับกิจกรรมการทำงานของนายหน้าประกันภัยแต่ละราย ซึ่งอาจแตกต่างกันไป รวมถึง การรวบรวมข้อมูล การเก็บข้อมูล การประมวลผล และการส่งข้อมูลต่างๆ

ทั้งนี้ แนวทางปฏิบัตินี้เป็นเพียงแต่แนวทาง หรือหลักการ ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น ส่วนนายหน้าประกันภัยแต่ละรายนั้นสามารถนำไปปรับปรุง ประยุกต์ใช้ตามความเหมาะสมกับการทำงาน และกิจกรรมของนายหน้าที่เกิดขึ้นจริง อีกทั้งแนวทางปฏิบัตินี้จะอ้างอิงถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เท่านั้น หากมีการปรับปรุงข้อกำหนด หรือมีประกาศ ข้อบังคับอื่นใด ในภายหลังที่มีผลต่อกิจกรรมการทำงานของนายหน้า ทางสมาคมจะแจ้งให้ท่านทราบ และขอให้ท่านพยายามศึกษาหาข้อมูลเพิ่มเติมต่อไป

ทางสมาคมนายหน้าประกันภัยไทย หวังเป็นอย่างยิ่งว่าแนวทางปฏิบัตินี้จะประโยชน์กับสมาชิกของสมาคมฯ และสามารถช่วยให้ท่านสามารถดำเนินธุรกิจได้อย่างมั่นคงและถูกต้อง

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ



(นายจิตวุฒิ ศศิบุตร)

นายกสมาคมนายหน้าประกันภัยไทย

สารบัญ

1. หลักการท้ไปเกี่ยวกับ กฎหมายค้คุมครองข้อมูลส่วนนุคคล (PDPA).....	3
1.1) ประเภทข้อมูลที่ได้รับความค้คุมครอง.....	3
1.2) ผู้ที่เกี่ยวข้กับข้อมูลส่วนนุคคล.....	4
1.3) ข้กำหนดสำคัญภายใต้กฎหมายค้คุมครองข้อมูลส่วนนุคคล ที่ต้องปฏิบัติตาม.....	4
1.4) ความแตกต่างระหว่าง ผู้ควบคุมข้อมูลส่วนนุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนนุคคล(Data Processor).....	5
1.5) หน้าทีและความรับผิดชอบตามมาตรา 37.....	6
2. นโยบายที่เกี่ยวข้กับการค้คุมครองข้อมูลส่วนนุคคลขององค์กร (Data Protection Policy).....	6
3. การบริหารจัดการข้อมูลส่วนนุคคล.....	8
4. หลักการเก็บข้อมูลเท่าทีจำเป็น (Data Minization).....	10
5. การประเมินผลกระทบด้านการค้คุมครองข้อมูลส่วนนุคคล (Data Protection Impact Assessment – DPIA).....	11
6. การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนนุคคล (Data Subject Right Request Management – DSRR).....	12
7. การก้กับดูแลหน่วยงานภายนอกการค้คุมครองข้อมูลส่วนนุคคล (Third Party Assessment).....	13
8. การจัดการเมื่อกิดเหตุละเมิดและการรั่วไหลของข้อมูลส่วนนุคคล (Incident and Breach Management)	13
9. บทสรุปรู หน้าทีของพนักงาน/บริษัท และหน้าทีของผู้บริหาร.....	16
10. อ้างอิงและข้จ้ก้ความรับผิดชอบ (Reference & Disclaimer)	16

ภาคผนวก

ตัวอย่างเอกสารและแบบฟอร์ม

1) ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) ส้หรับลูกค้้าใหม่.....	18
2) ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) ส้หรับลูกค้้าเดิม.....	19
3) ตัวอย่าง Data Sharing Agreement (DSA).....	20
4) ตัวอย่าง แบบฟอร์มคำร้องตามสิทธิของเจ้าของข้อมูลส่วนนุคคล.....	27

แนวทางปฏิบัติของนายหน้าประกันภัยนิติบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. หลักการทั่วไปเกี่ยวกับ กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

PDPA	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
วันที่ผลบังคับใช้	ตั้งแต่ 1 มิถุนายน 2565 เป็นต้นไป
หน่วยงานกำกับดูแล	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส)
ความรับผิด ในกรณีไม่ปฏิบัติตาม	<ul style="list-style-type: none"> ● โทษปรับสูงสุด 5 ล้านบาท ● โทษจำคุกสูงสุด 1 ปี ● ชดใช้ค่าเสียหายตามจริง รวมถึงค่าสินไหมทดแทนเพื่อการลงโทษสูงสุด 2 เท่า ● กรรมการ หรือ บุคคลซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล

1.1 ประเภทข้อมูลที่มีความคุ้มครอง

“ข้อมูลส่วนบุคคล” (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

- ชื่อ-นามสกุล หรือชื่อเล่น
- ที่อยู่ อีเมลล์ หมายเลขโทรศัพท์
- เลขที่ประจำตัวประชาชน, เลขที่หนังสือเดินทาง, เลขที่ประกันสังคม, เลขที่ใบอนุญาตขับขี่
- เลขที่บัญชีธนาคาร, เลขที่บัตรเครดิต
- ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID
- ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, เลขตัวถังรถยนต์, โฉนดที่ดิน
- ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (Location), ข้อมูลการศึกษา, ข้อมูลทางการเงิน
- ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
- ข้อมูลบันทึกต่างๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น log file

“ข้อมูลส่วนบุคคลที่ละเอียดอ่อน” (Sensitive Personal Data) เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน และเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
- พฤติกรรมทางเพศ

- ประวัติอาชญากรรม
- ข้อมูลการแพทย์ ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลทางชีวภาพ เช่น ข้อมูลสแกนลายนิ้วมือ, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง (Voice Recognition)
- หรือ ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

1.2 ผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1.2.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

บุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา ได้แก่

- ลูกค้า (Customer)
- ลูกค้าเป้าหมาย (Prospect Customer)
- พนักงาน
- ผู้ขาย / คู่ค้า
- อื่นๆ เช่น พนักงานที่ลาออกไปแล้ว

1.2.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม, ใช้, หรือเปิดเผยข้อมูลส่วนบุคคล

1.2.3 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม, ใช้, หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

1.3 ข้อกำหนดสำคัญภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่ต้องปฏิบัติตาม

1.3.1 ขอความยินยอม (Consent)

การจัดเก็บข้อมูลส่วนบุคคลที่ต้องพิจารณา “ขอความยินยอมจากเจ้าของข้อมูล (Data Subject) ก่อนหรือขณะที่เก็บข้อมูล”

1.3.2 การเก็บรักษา ข้อมูลส่วนบุคคล (Confidentiality & Security)

ต้องมีมาตรการเก็บรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัยและเป็นความลับ

1.3.3 สิทธิของเจ้าของข้อมูล (Right of the Data Subject)

มีกระบวนการ มาตรการรองรับการใช้สิทธิในข้อมูล ของเจ้าของข้อมูล (Data Subject)

1.3.4 มาตรการรักษา ส่งต่อ และแบ่งปันข้อมูล (Transfer)

มีมาตรการการรักษาความปลอดภัย ขณะ โอนหรือส่งต่อข้อมูล และการจัดทำสัญญาแบ่งปันข้อมูล

1.3.5 จัดเก็บ รักษา และบันทึก (Record of Processing)

จัดทำและเก็บรักษายันทึกรายการข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส) ตรวจสอบได้

1.3.6 สัญญาประมวลผลข้อมูล (Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ต้องเข้าทำสัญญาประมวลผลข้อมูล และปฏิบัติตามคำสั่งที่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

1.3.7 แนวทางปฏิบัติ เมื่อเกิดเหตุการณ์ ละเมิดข้อมูลส่วนบุคคล (Data Breach Notification)

Data Controller กำหนดแนวทางการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส) ภายใน 72 ชั่วโมง

1.3.8 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO – Data Protection Officer)

ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

1.4 ความแตกต่างระหว่าง ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

กิจกรรม	Data Controller	Data Processor
1. ผู้กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายที่ใช้ และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล	/	
2. ผู้กำหนดว่าต้องประมวลผลข้อมูลส่วนบุคคลของใครและพิจารณา ผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล	/	
3. เป็นผู้ได้รับประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลและมีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล	/	
4. เป็นผู้ทำการประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงหรือสัญญาที่ทำไว้กับเจ้าของข้อมูลส่วนบุคคลโดยตรง	/	
5. เป็นผู้แต่งตั้ง Data Processor เพื่อดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของบริษัท	/	
6. เป็นผู้ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของ Data Controller ภายใต้ข้อตกลง		/
7. เป็นผู้ที่ได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือจาก Data Controller และไม่เป็นผู้ที่ตัดสินใจเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล		/

หมายเหตุ

การตัดสินใจว่านายหน้าประกันภัยเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) นั้นจะขึ้นอยู่กับกิจกรรมของนายหน้าประกันภัยแต่ละรายที่มีต่อเจ้าของข้อมูล (Data Subject) และบุคคลที่สาม เช่น บริษัทประกันภัย ประกันชีวิต ฯลฯ

1.5 หน้าที่และความรับผิดชอบตามมาตรา 37

กิจกรรม	Data Controller	Data Processor
จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	/	/
ป้องกันไม่ให้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ	/	
จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล	/	
ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)	/	
มีบันทึกรายการของกิจกรรมการประมวลผลของข้อมูลส่วนบุคคล (Data Inventory)	/	/
มีกระบวนการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล	/	
ประเมินบุคคลภายนอกด้านความคุ้มครองข้อมูลส่วนบุคคล	/	/
ทำสัญญาประมวลผล (Data Processing Agreement) และสัญญาแบ่งปันข้อมูล (Data Sharing Agreement)	/	/
ดำเนินการให้มั่นใจว่าประเทศปลายทางที่โอนข้อมูลส่วนบุคคลไปให้มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ	/	/
สนับสนุนการปฏิบัติหน้าที่ของ DPO Office	/	/
ให้หน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลได้	/	/
แจ้งเหตุละเมิดข้อมูลส่วนบุคคล	แจ้ง ส.ค.ส ภายใน 72 ชั่วโมงนับแต่ทราบเหตุและแจ้งเจ้าของข้อมูล	แจ้ง Data Controller ภายใน 24 ชั่วโมง
ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือข้อมูลในสัญญาประมวลผลข้อมูล (DPA) กับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)		/
แจ้ง Data Controller กรณีพบการประมวลผลข้อมูลส่วนบุคคลที่ฝ่าฝืน PDPA		/
จัดเตรียมข้อมูลที่แสดงให้เห็นถึงการปฏิบัติตามข้อตกลงระหว่างบริษัท ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) กับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)		/
จัดเตรียมวิธีการในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล ตามวิธีการและข้อตกลงกับ Data Controller		/

2. นโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Data Protection Policy)

- นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)
- คู่มือการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Guideline for Data Protection Impact Assessment – DPIA)
- คู่มือการประเมินหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Third Party Assessment for Data Privacy Protection)

- คู่มือการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Guideline for Data Subject Right Request Management – DSRR)
- กฎบัตรการคุ้มครองข้อมูลส่วนบุคคล
- คู่มือการจัดการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล (Guideline for Incident and Breach Management)
- นโยบายความเป็นส่วนตัวสำหรับกล้องวงจรปิด (CCTV Notice), นโยบายการใช้คุกกี้ และนโยบายความเป็นส่วนตัว
- แนวทางการตรวจสอบ (Monitoring Program)

ผู้ที่เกี่ยวข้องกับ นโยบายและคู่มือ	Front Office	Back Office	DPO / Head of DPO
เมื่อมีกระบวนการหรือกิจกรรมใหม่เกิดขึ้น หรือต้องการทราบถึงการดำเนินงานด้าน PDPA เช่น ฐานกฎหมาย การเก็บ ใช้ ทำลายข้อมูลส่วนบุคคล	/	/	/
การดำเนินงานในระบบ IT หรือใช้งานอุปกรณ์ประมวลผลด้าน IT	/	/	
ทบทวนการจัดทำ DPIA อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อนำเทคโนโลยีใหม่มาใช้ประมวลผลข้อมูล	/	/	
เมื่อมีการจัดจ้าง Data Processor รายใหม่ หรือ Data Processor มีความเสี่ยงด้านการประมวลผลข้อมูล	/	/	
ได้รับคำร้องจากเจ้าของข้อมูล เช่น ลูกค้าขอเข้าถึง เปลี่ยนแปลง ลบข้อมูล	/	/	
มีการจัดตั้งเปลี่ยนแปลง Head of DPO/DPO Office			/
เกิดเหตุข้อมูลรั่วไหล ไปยังบุคคลภายนอก	/	/	/
มีการติดตั้ง CCTV / คุกกี้ ใหม่ หรือเมื่อมีการเก็บข้อมูลที่ไว้วัตถุประสงค์แตกต่างจากเดิม		/	/
การตรวจสอบการปฏิบัติงานให้เป็นไปตาม PDPA อย่างน้อยปีละ 1 ครั้ง			/

2.1 หน้าที่และความรับผิดชอบของ DPO

- ให้คำแนะนำ เกี่ยวกับการปฏิบัติงานในกระบวนการที่เกี่ยวข้องกับ PDPA ในบริษัท
- ติดตามตรวจสอบกระบวนการทำงานที่เกี่ยวข้องกับ PDPA และรายงานต่อ CEO
- ประสานงานและให้ความร่วมมือกับ ส.ค.ส และแจ้งเหตุการณ้ละเมิดข้อมูลส่วนบุคคล
- บริหารงานและกำกับดูแลงาน DPO Office
- จัดฝึกอบรมและนำเสนอข่าวสารเกี่ยวกับ PDPA
- ให้คำแนะนำเกี่ยวกับข้อบังคับทางกฎหมายและการจัดทำสัญญาหรือข้อตกลงกับหน่วยงานภายนอก

3. การบริหารจัดการข้อมูลส่วนบุคคล

3.1 การบริหารจัดการข้อมูลลูกค้า

กระบวนการกรอกข้อมูลโดย ลูกค้าแสดงความสนใจ

1	2	3	4	5
เก็บรวบรวม	ใช้	เปิดเผยหน่วยงานภายนอก	เก็บรักษา	ทำลาย
Registration Form - ชื่อ นามสกุล - เบอร์โทร / อีเมลล์ - พฤติกรรมการซื้อ ความสนใจ	- วิเคราะห์ข้อมูลลูกค้า Prospect เพื่อจัดกิจกรรมทางการตลาด - บันทึกรฐานข้อมูลลูกค้า - การส่งข้อความ SMS / Email / EDM	- บริษัทประกันภัย/ประกันชีวิต เพื่อปฏิบัติตามสัญญา - บริษัทสำรวจภัย / สถานพยาบาล เพื่อการบริการ	- ระบบ Server / Cloud / CRM - ตู้เก็บเอกสารของแผนก	- จัดจ้างหน่วยงานภายนอกที่รับทำลายเอกสาร - ทำลายเอกสารด้วยตัวเอง
ข้อควรพิจารณา				
*ขอความยินยอมจากเจ้าของข้อมูลก่อน หรือขณะเก็บข้อมูล *การขอความยินยอม อาจใช้เป็นเอกสาร หรือทางอิเล็กทรอนิกส์ *เก็บข้อมูลเท่าที่จำเป็น (ลบ ซีดฆ่า ข้อมูลอ่อนไหว - Sensitive Data)	*ดำเนินการ ได้เฉพาะรายที่ให้ ความยินยอม เท่านั้น และภายใต้วัตถุประสงค์ที่ได้แจ้ง	*เข้ารหัสทุกครั้งเมื่อมีการส่งข้อมูลส่วนบุคคลไปยังบุคคลภายนอกองค์กร *ส่งข้อมูลผ่านระบบ หรือช่องทางที่มีมาตรการรักษาความปลอดภัยอย่างเหมาะสม *เปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานบุคคลภายนอกที่ได้รับอนุญาตเท่านั้น	*เก็บเอกสารในตู้ที่สามารถล็อกได้ *กำหนดสิทธิ์การเข้าถึงข้อมูลในระบบ *ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล *เก็บตามระยะเวลาที่กฎหมายกำหนด / เท่าที่จำเป็น	*ทำลายเอกสารด้วยวิธีที่เหมาะสม เช่น เครื่องย่อยเอกสาร เป็นต้น *มีระบบ / กระบวนการตรวจสอบเพื่อทำลายข้อมูล *ระบุข้อตกลงที่จำเป็นในสัญญาจ้างหน่วยงานภายนอกอย่างเหมาะสม และขอหลักฐานการทำลายเอกสาร เช่น รูปภาพ เป็นต้น

3.2 การบริหารจัดการข้อมูลพนักงาน

กระบวนการกรอกข้อมูลพนักงานในองคักร

1	2	3	4	5
เก็บรวมรวม	ใช้	เปิดเผยหน่วยงานภายนอก	เก็บรักษา	ทำลาย
ใบสมัครงาน / สัญญาจ้าง - ชื่อ นามสกุล - ที่อยู่เบอร์โทร / อีเมลล์ - เพศ - วันเกิด อายุ - บัศรประชาชน - เงินเดือน เลขที่บัญชี	- จัดทำเงินเดือนพนักงาน - จัดทำหนังสือรับรองการหักภาษี - จัดทำ กงค.1 - จัดสวัสดิการพนักงาน	- ฝ่ายบัญชี เพื่อบันทึกบัญชี - กรมสรรพากร เพื่อยื่นภาษี - เพื่อส่งให้บริษัทประมวลผล/ คำนวณผลประ โยชน์พนักงาน - บริษัทประกันกัฒน / ประกันชีวิต / สถานพยาบาล เพื่อการบริการ	- ระบบ Server / Cloud - ระบบบริหารงานบุคคล (HR) - ผู้เก็บเอกสารของแผนก	- จัดจ้างหน่วยงานภายนอกที่รับทำลายเอกสาร - ทำลายเอกสารด้วยตัวเอง
ข้อควรพิจารณา				
*ขอความยินยอมจากพนักงานก่อนหรือขณะทีเก็บข้อมูล *เก็บข้อมูลเท่าทีจำเป็น ใบสัญญาจ้างงาน/ใบสมัครงาน	*ใช้ตามวัตถุประสงค์ในการประมวลผลข้อมูลตามสัญญาหรือทีได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้น	*เข้ารหัสทุกครั้งเมื่อมีการส่งข้อมูลส่วนบุคคลไปยังบุคคลภายนอกองคักร *ส่งข้อมูลผ่านระบบ หรือช่องทางทีมีมาตรการรักษาความปลอดภัยอย่างเหมาะสม *เปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานบุคคลภายนอกตามที่ได้รับการยินยอมจากเจ้าของข้อมูลเท่านั้น	*เก็บเอกสารในดู่ทีสามารถลือกได้ *กำหนดสิทธิ์การเข้าถึงข้อมูลในระบบ *ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล *เก็บตามระยะเวลาทีกฎหมายกำหนด / เท่าทีจำเป็น	*ทำลายเอกสารด้วยวิธีทีเหมาะสม เช่น เครื่องย่อยเอกสาร เป็นต้น *มีระบบ / กระบวนการตรวจสอบเพื่อทำลายข้อมูล *ระบุข้อตกลงทีจำเป็นในสัญญาจ้างหน่วยงานภายนอกอย่างเหมาะสม และขอหลักฐานการทำลายเอกสาร เช่น รูปภาพ เป็นต้น

4. หลักการเก็บข้อมูลที่จำเป็น (Data Minimization)

อ้างอิง “พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา22 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

จัดเก็บข้อมูลที่จำเป็น : เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูล

จัดเก็บข้อมูลที่เกี่ยวข้อง : เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการประมวลผลข้อมูล

จัดเก็บข้อมูลที่จำกัดเฉพาะ : เก็บรวบรวมข้อมูลส่วนบุคคลในปริมาณที่จำกัดเฉพาะสำหรับการใช้ประมวลผลข้อมูลเท่านั้น และเก็บรักษาข้อมูลตามระยะเวลาที่จำเป็นเพื่อการประมวลผล หรือตามที่กฎหมายกำหนด

แนวทางการปฏิบัติเพื่อให้เป็นไปตามหลักการเก็บข้อมูลที่จำเป็น จำแนกตามรูปแบบข้อมูล

1. ทางเอกสาร

- **ปิดทับข้อมูลที่ไม่จำเป็น** ให้ไม่สามารถมองเห็นหรืออ่านข้อมูลได้ ในกรณีที่มีความจำเป็นต้องขอเอกสารที่มีข้อมูลประเภทนั้น
- **ปรับปรุงแบบฟอร์ม** การรวบรวมข้อมูลใหม่ กรณีที่แบบฟอร์มนั้นๆ มีช่องให้กรอกข้อมูลที่ไม่จำเป็นต้องใช้สำหรับกรณีดังกล่าว
- **ทำลายเอกสาร** เมื่อไม่มีความจำเป็นต้องใช้ หรือเก็บรักษา

2. ทางอิเล็กทรอนิกส์

- **กำหนดคำสั่ง** หรือฟังก์ชันในระบบ ให้บันทึกและจัดเก็บเฉพาะข้อมูลที่จำเป็น สำหรับวัตถุประสงค์ในการประมวลผล และแจ้งเตือนเมื่อครบกำหนด ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- **พิจารณาใช้ Aggregated Data** เช่น ข้อมูลทางสถิติ ซึ่งไม่ถือเป็นข้อมูลส่วนบุคคล ในการประมวลผลตามวัตถุประสงค์ของกิจกรรม ถ้าสามารถทำได้
- **ตั้งค่าในระบบให้ไม่ต้องมี Field** ในการกรอกข้อมูลที่ไม่มีความจำเป็นต้องใช้
- **ปิดทับข้อมูล** ที่ไม่จำเป็นในไฟล์แนบ ให้ไม่สามารถมองเห็นหรืออ่านข้อมูลก่อนจัดเก็บหรือส่งต่อ
- **ลบ Email** เมื่อไม่มีความจำเป็นต้องใช้
- **ลบข้อมูล** ใน Shared Drive, Personal Drive, Server หรือ System ที่เกี่ยวข้อง และ/หรือ อุปกรณ์อิเล็กทรอนิกส์ เช่น แฟลชไดรฟ์ ฮาร์ดดิสก์ และคอมพิวเตอร์ส่วนตัว เมื่อไม่มีความจำเป็นต้องใช้หรือเก็บรักษา
- **จัดทำข้อมูลนิรนาม (Anonymization)*** เช่น การสลับลำดับของตัวอักษรบนข้อมูล (Scrambling) หรือการปิดทับข้อมูล (Masking) เป็นต้น
- **การแฝงข้อมูลส่วนบุคคล (Pseudonymization) หรือการขจัดตัวตน (De-identification)** โดยการเปลี่ยนข้อมูลที่ระบุตัวตนด้วยข้อมูลอื่นๆ หรือเลขที่กำหนดใหม่ขึ้นมา

ตัวอย่างข้อมูลส่วนบุคคลที่ไม่จำเป็น และไม่มีความเกี่ยวข้องกับวัตถุประสงค์การประมวลผลข้อมูล

ตัวอย่างกิจกรรมการประมวลผล ข้อมูลส่วนบุคคล	ตัวอย่างข้อมูลส่วนบุคคลที่ไม่จำเป็น
- แจกการทำประกันรถยนต์ - รับชำระเบี้ยประกันภัย	- รายละเอียดในบัตรประชาชน เช่น กรุ๊ปเลือด ศาสนา
- การรับข้อมูลผู้สมัครงาน	- รายละเอียดในบัตรประชาชน เช่น กรุ๊ปเลือด ศาสนา - ข้อมูลครอบครัว – อายุ สถานะสมรสบิดามารดา อาชีพ ตำแหน่ง บริษัทที่ทำงาน ของบิดา มารดา พี่น้อง
- การบันทึกข้อมูลลูกค้าซื้อประกัน	- สำเนาบัตรเครดิต - รายละเอียดในบัตรประชาชน เช่น กรุ๊ปเลือด ศาสนา
- การเบิกเงินสดย่อย / เงินทวงจ่าย	- รายละเอียดในบัตรประชาชน เช่น กรุ๊ปเลือด ศาสนา - เอกสารประกอบการเบิกเงินสดย่อยที่มีข้อมูลส่วนบุคคล เมื่อส่งให้แผนกบัญชีและการเงินเรียบร้อยแล้ว

5. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment – DPIA)

เป็นกระบวนการที่ออกแบบเพื่อช่วยในการวิเคราะห์ ระบุ และลดความเสี่ยง เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละกิจกรรมได้อย่างเป็นธรรมชาติ

บริษัทฯ ควรจัดทำหรือประเมิน DPIA เมื่อ “กิจกรรมการประมวลผลข้อมูลส่วนบุคคล ที่สามารถส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างมาก”

ผู้ที่มีส่วนร่วมในกิจกรรม DPIA ได้แก่

- เจ้าของกิจกรรมประมวลผลข้อมูล (Process Owner)
- DPO (Data Protection Officer)
- บุคลากรด้านความมั่นคงปลอดภัยทางสารสนเทศ (IT Security)
- ผู้ประมวลผล (Data Processor)

DPIA เป็นกระบวนการที่สำคัญและจำเป็นต้องจัดทำตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4, 30, 37, 39 และ 40 โดยระบุถึงขั้นตอนที่ต้องทราบถึง ผลกระทบและมาตรการควบคุมที่เหมาะสมเพื่อลดผลกระทบและความเสี่ยง

*หากไม่ปฏิบัติตาม จะมีบทลงโทษ โดย ชด ใช้ค่าเสียหายตามจริง รวมถึงค่าสินไหมทดแทนเพื่อการลงโทษสูงสุด 2 เท่า โทษปรับ สูงสุด 3 ล้านบาท

กระบวนการที่ควรคำนึงถึง เมื่อจัดทำ DPIA

1. อธิบายรายละเอียดของกระบวนการประมวลผล ข้อมูลส่วนบุคคล
2. ขอคำปรึกษาจากผู้ที่เกี่ยวข้อง
3. ประเมินความจำเป็นของการประมวลผลข้อมูลส่วนบุคคล
4. ประเมินความเสี่ยงและผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
5. ระบุมาตรการเพื่อลดความเสี่ยงของกิจกรรม พร้อมขอคำปรึกษาจาก DPO
6. สรุปผลการประเมิน DPIA และรายงานต่อผู้ที่มีอำนาจเพื่อดำเนินการอนุมัติ
7. ติดตาม ตรวจสอบ และทบทวนการจัดทำ DPIA

6. การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Request Management – DSRR)

กระบวนการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่ PDPA กำหนด คำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และการบริหารจัดการข้อสอบถามและข้อร้องเรียนที่เกี่ยวข้องกับคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อได้รับคำร้อง และดำเนินการให้แล้วเสร็จ โดยไม่ชักช้า ภายใน 30 วัน หรือตามที่บริษัทกำหนด

ผู้ที่เกี่ยวข้องกับการรับคำร้องได้แก่

- หน่วยงานที่เกี่ยวข้องกับการรับคำร้อง
- หน่วยงานที่เป็นเจ้าของกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Process Owner)
- หน่วยงานคุ้มครองข้อมูลส่วนบุคคล (DPO)
- ฝ่ายกฎหมาย
- ผู้ประมวลผลข้อมูล (Data Processor)

*มาตรา 82 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใด ไม่ปฏิบัติตามมาตรา 30 วรรค 4 ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

6.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิในการถอนความยินยอม, การลบ, การระงับ ข้อมูลส่วนบุคคล
- สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
- สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล
- สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล

6.2 ขั้นตอนในการจัดการคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

1. การรับคำร้องของเจ้าของข้อมูลส่วนบุคคล
2. การยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3. การพิจารณาคำร้อง
4. การแจ้งยืนยันเพื่อดำเนินการตามคำร้อง

5. การดำเนินการตามคำร้อง
6. การปิดสถานะคำร้องเมื่อเสร็จสิ้นการดำเนินการ
7. การติดตามสถานะและการดำเนินการตามคำร้อง

7. การกำกับดูแลหน่วยงานภายนอกด้านการคุ้มครองข้อมูลส่วนบุคคล (Thrid-Party Assessment)

7.1 การกำกับดูแลหน่วยงานภายนอก

➤ การทำสัญญา (Contractual)

โดยระบุหน่วยงานภายนอกที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล หรือใช้ข้อมูลส่วนบุคคลร่วมกันเพื่อลงนามข้อตกลง เช่นการทำสัญญารักษาความลับ และสัญญาประมวลผล หรือถ่ายโอนข้อมูลระหว่าง บริษัทนายหน้า และบริษัท ประกันภักภ/ประกันชีวิต

➤ การประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล (Assessment of Data Privacy Protection)

ประเมินความเสี่ยงของ Data Processor ในด้านการคุ้มครองข้อมูลส่วนบุคคล

➤ การตรวจสอบ (Assurance)

ตรวจสอบการปฏิบัติตามกระบวนการทำสัญญา และประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล

7.2 ประเมินความเสี่ยงของ Data Processor ในด้านการคุ้มครองข้อมูลส่วนบุคคลก่อนดำเนินการจัดซื้อจัดจ้าง หรือก่อนส่ง หรือ โอนข้อมูลส่วนบุคคลไปให้ (หรือเป็นไปตามสัญญา/คำสั่ง ในนาม Data Controller ภายใต้ข้อตกลง และไม่ได้เป็นผู้ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

ตัวอย่าง บุคคลภายนอกที่ควรประเมิน เช่น ผู้รับจ้างดูแลระบบคอมพิวเตอร์, ผู้ให้บริการรับฝาก / เก็บข้อมูลส่วนบุคคล, บริษัทรับจ้างส่ง SMS, บริษัทรับทำเงินเดือน, รับจ้างต่อ Visa หรือ Work Permit, บริษัทจัดหางาน, โรงพยาบาล เป็นต้น

8. การจัดการเมื่อเกิดเหตุละเมิดและรั่วไหลของข้อมูลส่วนบุคคล (Incident and Breach Management)

เมื่อเกิดเหตุละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล เช่นการเข้าถึง การเปิดเผย การเปลี่ยนแปลง การทำซ้ำ ข้อมูลส่วนบุคคล ซึ่งทำให้เกิดผลเสียหายต่อข้อมูลส่วนบุคคล โดยมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลต้องเชื่อมโยงไป เช่น

- การถูกเลือกปฏิบัติ
- การถูกสวมรอยบุคคลหรือถือ โกง
- ทำให้เกิดความเสียหายทางการเงิน การเสียชื่อเสียง
- การถูกเปิดเผยข้อมูลส่วนบุคคลที่ต้องคุ้มครองตามมาตราการรักษาความลับทางวิชาชีพ
- การถอดรหัสข้อมูลแฝงโดยไม่ได้รับอนุญาต
- การเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญ

8.1 ระเบวนการจัการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล

8.1.1 เหตุละเมิดที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ (IT)

- เกิดภันคุกคามด้านไซเบอร์ (Cyber Attack)
- เหตุละเมิดที่เกี่ยวกับอุปกรณ์อิเล็กทรอนิกส์ด้าน IT ที่ใช้รวบรวมและประมวลผลข้อมูลส่วนบุคคล

8.1.2 เหตุละเมิดที่ไม่เกี่ยวข้องกัระบบเทคโนโลยีสารสนเทศ (Non-IT)

- เหตุละเมิด ที่เกิดจากมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical Security) ในการเก็บข้อมูลส่วนบุคคลที่อยู่ในรูปแบบเอกสารที่ไม่เพียงพอ
- เหตุละเมิดที่เกิดจากเหตุสุควิสัย หรือภันพิบัติทางธรรมชาติ

8.1.3 หน่วยงานที่เป็นเจ้าของระเบวนการ (Process Owner)

- หน่วยงานที่รับผิดชอบจัการแก้ไขเหตุละเมิด หรือมีหน้าที่ดำเนินการสืบสวน วิเคราะห์หาสาเหตุ ประเมินผลกระทบต้อเจ้าของข้อมูลส่วนบุคคล และจัทำแผนการแก้ไข และแนวทางเยียวยา ภันที่เหตุละเมิด ที่มีผลกระทบต้อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

8.2 การแจ้งเหตุละเมิดและบุคคลที่เกี่ยวข้อง

แจ้งเหตุละเมิดฯแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส.) ภายใน 72 ชั่วโมง (นับแต่ทราบเหตุเท่าที่สามารถทำได้) หากเหตุละเมิด ดังกล่าวมีความเสี่ยงกระทบต้อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (มาตรา 37 (4))

โดยมีบุคคลที่เกี่ยวข้องได้แก่

- หน่วยงานที่รับแจ้งเหตุละเมิด
- หน่วยงานที่เกี่ยวข้อง
- เจ้าหน้าที่และหน่วยงานคุ้มครองข้อมูลส่วนบุคคล (DPO)
- ฝ่ายเทคโนโลยีสารสนเทศ (IT)
- ฝ่ายกฎหมาย
- ผู้ประมวลผล (Data Processor)

*มาตรา 83 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใด ไม่ปฏิบัติตามมาตรา 37 ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

8.3 5 ขั้นตอนในการจัการเหตุละเมิดและการรั่วไหลของข้อมูลส่วนบุคคล

1. การตรวจพบ สืบสวน และวิเคราะห์ผลกระทบของเหตุละเมิด
2. การจัทำแผนการแก้ไขและแนวทางการเยียวยาแก่ผู้ที่ได้รับผลกระทบ
3. แจ้งเหตุละเมิด ต้อ ส.ค.ส และบุคคลอื่นๆ (บริษัทประกันภัน) ที่ถูกระบุด้วยสัญญา
4. การติดตาม รายงานผลการแก้ไข และปิดสถานะเหตุละเมิด
5. สอบทาน และทบทวนระเบวนการจัการเหตุละเมิด โดย DPO

8.4 ระยะเวลาการดำเนินการ / แก้ไขเหตุละเมิด (SLA)

ประเภทการแจ้งเหตุละเมิด	ระยะเวลาดำเนินการ
เหตุละเมิดฯ ที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล	- รายงานต่อ ส.ค.ส ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ - ระยะเวลาแก้ไขขึ้นอยู่กับความรุนแรงผลกระทบที่บริษัท กำหนดในนโยบายการรักษาความมั่นคงปลอดภัยทาง สารสนเทศ (IT Security)
เหตุละเมิดฯ ที่ไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล	ระยะเวลาแก้ไขขึ้นอยู่กับความรุนแรงผลกระทบที่บริษัท กำหนดในนโยบายการรักษาความมั่นคงปลอดภัยทาง สารสนเทศ (IT Security)
ตอบคำถาม / ข้อเสนอของเหตุละเมิด จาก ส.ค.ส หรือเจ้าของข้อมูลส่วนบุคคล	ภายใน 48 ชั่วโมง นับตั้งแต่ได้รับการติดต่อ

ตัวอย่างการดำเนินการหลังเกิดเหตุละเมิด

บริษัทนายหน้าประกันภัยแห่งหนึ่งถูกเจาะเข้าถึงระบบรักษาความปลอดภัย ส่งผลให้การเข้าเว็บไซต์ของนายหน้าประกันภัยรายนั้นถูกเปลี่ยน ไปยังเว็บไซต์หลอกลวง ซึ่งทำให้ข้อมูลส่วนบุคคลและข้อมูลการเงินของลูกค้ารั่วไหล ประมาณ 5,000 ราย

ข้อมูลที่รั่วไหล ได้แก่ ชื่อ-นามสกุล, ที่อยู่, อีเมลล์, อายุ, ข้อมูลรถยนต์, เลขบัตรประชาชน, เลขบัตรเครดิต, รหัส CVC (Card Verification Code) และ CVV (Card Verification Value)

การดำเนินการ

1. แจ้งลูกค้า
2. แจ้งหน่วยงานที่เกี่ยวข้อง
3. แนะนำลูกค้าเปลี่ยนรหัสผ่าน
4. ชดใช้ค่าสินไหมทดแทน แก่ ลูกค้า
5. เฝ้าระวังรายการที่น่าสงสัย

มาตรการป้องกัน

- ดำเนินการทดสอบด้านความปลอดภัยของ Application ใหม่ ก่อนนำมาใช้จริง
- ตรวจสอบ เปลี่ยนแปลง ระบบ Network ต่างๆ ให้มีความมั่นคงปลอดภัยมากขึ้น
- เฝ้าระวังติดตามตรวจสอบความปลอดภัยเป็นระยะๆ
- ปรับปรุงนโยบาย และแนวปฏิบัติ ในเรื่องความมั่นคงปลอดภัยทางสารสนเทศ (IT Security) ของบริษัทฯ

9. บทสรุป

หน้าที่ของ พนักงาน / บริษัท

- 1) จัดเก็บข้อมูลส่วนบุคคลอย่างเหมาะสม
 - ขอความยินยอมจากลูกค้า / พนักงาน
 - เก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น
 - จัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลตามระยะเวลาที่บริษัทกำหนด
 - ทำลายเอกสารอย่างเหมาะสม
 - ทบทวนและปรับปรุง Data Inventory ให้เป็นปัจจุบันอย่างสม่ำเสมอ
- 2) ประเมิน DPIA เมื่อมีกิจกรรมใหม่ หรือเมื่อมีการเปลี่ยนแปลงกิจกรรมอย่างมีนัยสำคัญ
- 3) ดำเนินการตามคำร้องขอของเจ้าของข้อมูล
- 4) กำกับดูแลหน่วยงานภายนอก
 - ประเมินผู้ประมวลผลข้อมูลด้านการคุ้มครองข้อมูลส่วนบุคคลและทบทวนการประเมินประจำปี
 - จัดทำสัญญาประมวลผลข้อมูลกับผู้ประมวลผลข้อมูลและสัญญาแบ่งปันข้อมูลกับผู้ควบคุมข้อมูลรายอื่น (บริษัท ประกันภัย/ประกันชีวิต เป็นต้น)
- 5) ปฏิบัติตาม IT Security Policy อย่างเคร่งครัด และจัดให้มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเมื่อโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
- 6) สนับสนุนการปฏิบัติหน้าที่ของ DPO และหน่วยงานรัฐ
- 7) แจ้งไปยัง DPO และผู้ปฏิบัติงานที่เกี่ยวข้องให้ทราบทันที เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

หน้าที่ของ ผู้บริหาร

สนับสนุนให้มีทรัพยากรอย่างเพียงพอ จัดทำให้มีนโยบายความมั่นคงปลอดภัยของข้อมูล และสารสนเทศ รวมถึงสร้างการตระหนักเรื่องการคุ้มครองข้อมูลส่วนบุคคลให้แก่พนักงาน

10. อ้างอิง และข้อจำกัดความรับผิดชอบ (Reference & Disclaimer)

สมาคมนายหน้าประกันภัยไทย รวมถึงกรรมการของสมาคมฯทุกคน มีความตั้งใจที่จะแบ่งปันให้ความรู้เกี่ยวกับพระราชบัญญัติข้อมูลส่วนบุคคล ฉบับ พ.ศ. 2562 แก่สมาชิกสมาคมนายหน้าประกันภัยไทย ซึ่งได้รวบรวมข้อมูลจากแหล่งต่างๆ และนำมาสรุปโดยเน้นย้ำประเด็นหลักๆเท่านั้น เพื่อให้ง่ายแก่ความเข้าใจและสามารถนำไปปฏิบัติใช้ได้จริงภายในเวลาที่จำกัด ทางสมาคมฯมิได้มีจุดประสงค์ในการแสวงหาผลตอบแทนอื่นใด แต่ทั้งนี้หากข้อความ เนื้อหา ความผิดพลาดหรือความที่ไม่ทันต่อสถานการณ์ รวมถึงผลของกฎหมายประกอบอื่นๆ ที่มีนั้น ทางสมาคมฯจะไม่รับผิดชอบต่อความเสียหายใดๆที่เกิดขึ้น หรือในทางกฎหมายอื่นใด โดยถือว่าสมาชิกของสมาคมฯ รวมถึงบุคคลทั่วไป ควรใช้วิจารณญาณ และศึกษาข้อมูลอื่นๆประกอบ ในการนำไปใช้ เพื่อปฏิบัติตามพระราชบัญญัติข้อมูลส่วนบุคคล ฉบับ พ.ศ. 2562 ดังกล่าว

ภาคผนวก

ตัวอย่างเอกสารและแบบฟอร์ม

เอกสารที่แนบมานี้ เป็นเพียงตัวอย่าง นายหน้าแต่ละราย อาจนำไปปรับปรุงให้เหมาะสมกับกิจกรรม นโยบาย และข้อมูลที่ต้องการหรือจัดเก็บ ตามความเหมาะสม

- 1) ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) สำหรับลูกค้าใหม่
- 2) ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) สำหรับลูกค้าเดิม
- 3) ตัวอย่าง Data Sharing Agreement (DSA)
- 4) ตัวอย่าง แบบฟอร์มคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

1. ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) สำหรับลูกค้าใหม่

(หัวข้อคหามยของบริษัทฯ)

หนังสือให้ความยินยอมในการเก็บและใช้ข้อมูล

เรียน [ลูกค้า]

บริษัท _____ จำกัด (“บริษัทฯ”) ใค้ขอความยินยอมจากท่านในการเก็บและใช้ข้อมูลส่วนนุคคของท่าน เพื่อวัตถุประสงค์ดังต่อไปนี้

ความยินยอมเกี่ยวกับการพัฒนาบริการ และการนำเสนอข่าวสารและบริการของบริษัทฯ

เก็บและใช้ข้อมูลส่วนนุคคของท่านเพื่อสำรวจความพึงพอใจของท่านเกี่ยวกับบริการของบริษัทฯ และวิเคราะห์ความสนใจของท่านและข้อมูลประวัติการใช้จ่ายหรือการใช้บริการ เพื่อประเมิน ปรับปรุง และพัฒนาบริการ และรายการส่งเสริมการขายต่าง ๆ ของบริษัทฯ ให้ตรงตามความต้องการของท่าน ได้ดียิ่งขึ้น และเพื่อแจ้งข้อมูลหรือแจ้งเตือนใด ๆ เกี่ยวกับบริการที่ท่านมีอยู่กับบริษัทฯ รวมถึงบริการอื่น ๆ สิทธิประโยชน์ รายการส่งเสริมการขายต่าง ๆ กิจกรรมทางการตลาด การเชิญชวนเข้าร่วมงานกิจกรรม และนำเสนอบริการต่าง ๆ ของบริษัทฯ ให้ท่านทราบผ่านทาง [โทรศัพท์ / ข้อความ SMS / E-mail]

โปรดศึกษารายละเอียดเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนนุคคตามนโยบายความเป็นส่วนตัวของบริษัทฯ [ที่ปรากฏตามเอกสารแนบ]

ท่านสามารถยกเลิกความยินยอมที่ท่านให้ไว้ได้ทุกเมื่อ โดยแจ้งบริษัทฯ ได้ที่ [โปรดระบุช่องทางการถอนความยินยอม เช่น Call center, E-mail, website]

สำหรับลูกค้า

วันที่ _____ เดือน _____ พ.ศ. _____

ชื่อ-นามสกุล _____

เลขประจำตัวประชาชน/เลขที่หนังสือเดินทาง _____

ข้าพเจ้าได้อ่านและเข้าใจวัตถุประสงค์ข้างต้น รวมทั้ง นโยบายความเป็นส่วนตัวของบริษัทฯ โดยตลอดแล้ว จึงตกลงและให้ความยินยอมแก่บริษัทฯ ในการเก็บและใช้ข้อมูลส่วนนุคคของข้าพเจ้าตามวัตถุประสงค์ข้างต้นทุกประการ

ยินยอม

ไม่ยินยอม*

ลงชื่อ _____ เจ้าของข้อมูล

(_____)

หมายเหตุ* หากท่านไม่ให้ความยินยอมข้างต้น ท่านยังคงสามารถติดต่อกับบริษัทฯ ได้อยู่ภายใต้สัญญาหรือนิติสัมพันธ์ที่ท่านมีอยู่กับบริษัทฯ แต่ท่านอาจไม่ได้รับความสะดวกหรือเสียสิทธิประโยชน์ที่ท่านอาจได้รับในอนาคตสำหรับกรณีอื่น ๆ [โปรดแจ้งค่าเตือนอื่น ๆ กรณีที่ไม่ให้ความยินยอม (ถ้ามี)]

2. ตัวอย่าง ฟอร์มขอความยินยอม (Consent Form) สำหรับลูกค้าเดิม

(หัวข้อหมายของบริษัทฯ)

วันที่

เรื่อง วัตถุประสงค์การเก็บและใช้ข้อมูลส่วนบุคคลของท่าน

เรียน

อ้างถึง [โปรดระบุบริการที่เกี่ยวข้อง]

บริษัท _____ จำกัด (“บริษัทฯ”) ตระหนักถึงความสำคัญในการดูแลข้อมูลส่วนบุคคลของท่านภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้องเป็นอย่างดี

เพื่อความโปร่งใสและเพื่อให้ บริษัทฯ ยังคงสามารถนำเสนอบริการที่เหมาะสมกับท่าน รวมถึงนำเสนอทางเลือกที่อาจเป็นประโยชน์ต่อท่านได้มากที่สุดอย่างต่อเนื่อง บริษัทฯ จึงมีความประสงค์จะเรียนให้ท่านทราบว่า ปัจจุบัน บริษัทฯ ได้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่าน เพื่อวัตถุประสงค์ดังต่อไปนี้

- เพื่อสำรวจความพึงพอใจของท่านเกี่ยวกับบริการของบริษัทฯ และวิเคราะห์ความสนใจของท่านและข้อมูลประวัติการใช้งานหรือการใช้บริการ เพื่อประเมิน ปรับปรุงและพัฒนา บริการ และรายการส่งเสริมการขายต่าง ๆ ของบริษัทฯ ให้ตรงตามความต้องการของท่านได้ดียิ่งขึ้น
- เพื่อแจ้งข้อมูลหรือแจ้งเตือนใด ๆ เกี่ยวกับบริการที่ท่านมีอยู่กับบริษัทฯ รวมถึงบริการอื่น ๆ สิทธิประโยชน์ รายการส่งเสริมการขายต่าง ๆ กิจกรรมทางการตลาด การเชิญชวนเข้าร่วมงานกิจกรรม และนำเสนอบริการต่าง ๆ ของบริษัทฯ ให้ท่านทราบผ่านทาง [โทรศัพท์ / ข้อความ SMS / E-mail]

บริษัทฯ ขออนุญาตดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านตามวัตถุประสงค์ข้างต้นต่อไปและตามที่ระบุไว้ในนโยบายความเป็นส่วนตัวของบริษัทฯ ทั้งนี้ เพื่อประโยชน์สูงสุดของท่าน โปรดศึกษารายละเอียดเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ ที่นโยบายความเป็นส่วนตัว [\[URL หน้าเว็บไซต์\]](#)

หากท่านมีข้อสงสัยหรือไม่ประสงค์ให้บริษัทฯ เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านสำหรับวัตถุประสงค์ที่ได้ระบุดังกล่าวข้างต้นอีกต่อไป ท่านสามารถติดต่อสอบถามหรือแจ้งความประสงค์ในการถอนความยินยอมได้ที่ [โปรดระบุช่องทางการติดต่อ เช่น call center อีเมล]

ขอแสดงความนับถือ

()

3. ตัวอย่างสัญญาแบ่งปันข้อมูล (Data Sharing Agreement)

ตัวอย่างสัญญาแบ่งปันข้อมูล

สัญญาแบ่งปันข้อมูลฉบับนี้ (“สัญญา”) ทำขึ้นเมื่อวันที่ [] ระหว่าง

บริษัท _____ จำกัด ซึ่งเป็นบริษัทจำกัดจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย โดยมีทะเบียนนิติบุคคลเลขที่ _____ และมีสำนักงานตั้งอยู่เลขที่ _____ (“_____”) ฝ่ายหนึ่ง กับ

[ชื่อบริษัท] [ซึ่งเป็นบริษัทจำกัดจดทะเบียนจัดตั้งขึ้นตามกฎหมายของประเทศไทย] โดยมีทะเบียนนิติบุคคลเลขที่ [] และมีสำนักงานตั้งอยู่เลขที่ [] (“บริษัทฯ”) อีกฝ่ายหนึ่ง

ในสัญญาฉบับนี้ คำว่า “คู่สัญญาฝ่ายหนึ่ง” หมายถึง มิลเลนเนียม ออโต้ หรือบริษัทฯ เพียงฝ่ายหนึ่งฝ่ายใด หากเป็นกรณีที่หมายถึงคู่สัญญาทั้งสองฝ่ายจะใช้คำว่า “คู่สัญญา”

โดยที่

(1) คู่สัญญาได้ตกลงทำสัญญา **[ชื่อสัญญาหลัก]** (“สัญญาหลัก”) เมื่อวันที่ **[วันที่ทำสัญญาหลัก]** ซึ่งคู่สัญญาจะต้องแบ่งปันข้อมูลส่วนบุคคลระหว่างกันในการปฏิบัติหน้าที่ตามสัญญาหลัก

(2) คู่สัญญาทั้งสองฝ่ายตกลงใช้ข้อมูลส่วนบุคคลที่แบ่งปันกันตามวัตถุประสงค์ที่ได้ตกลงกัน (ตามรายละเอียดที่ปรากฏในเอกสารแนบท้าย 1) ภายใต้ข้อตกลงและเงื่อนไขของสัญญาฉบับนี้ โดยคู่สัญญาแต่ละฝ่ายต่างมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

คู่สัญญาจึงตกลงกันดังต่อไปนี้

1. คำนิยามและการตีความ

1.1 หากไม่ได้มีการกำหนดไว้เป็นอย่างอื่นในสัญญาฉบับนี้ให้ถือคำในสัญญาฉบับนี้ มีความหมายดังต่อไปนี้

“ผู้ควบคุมข้อมูล” หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้เปิดเผยข้อมูล” หมายถึง คู่สัญญาฝ่ายหนึ่งซึ่งเปิดเผยหรือแบ่งปันข้อมูลส่วนบุคคลที่ถูกแบ่งปันให้แก่คู่สัญญาอีกฝ่ายหนึ่ง

“ผู้ประมวลผลข้อมูล” หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูล

“กฎหมายคุ้มครองข้อมูลส่วนบุคคล” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึง ฉบับแก้ไขเพิ่มเติม กฎระเบียบ ประกาศ และคำสั่ง ที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

“ผู้รับข้อมูล” หมายถึง คู่สัญญาฝ่ายหนึ่งซึ่งได้รับข้อมูลส่วนบุคคลที่ถูกแบ่งปันจากผู้เปิดเผยข้อมูล

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดาผู้ที่มีข้อมูลส่วนบุคคลนั้นบ่งชี้ไปถึง และให้หมายรวมถึง ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้โอนบุคลากรที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ

“การรั่วไหลของข้อมูลส่วนบุคคล” หมายถึง การรั่วไหลหรือละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ทำให้เกิดการประมวลผล เข้าถึง เปิดเผย ทำสำเนา เปลี่ยนแปลง เก็บ ทำซ้ำ แสดง หรือจำหน่ายข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย หรือทำให้เกิดการสูญหาย ทำลาย

เปลี่ยนแปลง หรือเสียหายต่อข้อมูลส่วนบุคคลที่ผู้รับข้อมูล และ/หรือ ผู้รับจ้างช่วงได้ดำเนินการส่ง เก็บ หรือประมวลผลในประการอื่นอันเกี่ยวข้องกับสัญญาหลักโดยอุบัติเหตุหรือโดยไม่ชอบด้วยกฎหมาย

“การประมวลผลข้อมูล” หมายถึง การกระทำการใด ๆ ต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย รวมถึงการอื่นใดที่ถูกควบคุมโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล

“หน่วยงานกำกับดูแล” หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย หรือหน่วยงานกำกับดูแลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอื่นซึ่งมีอำนาจในอาณาเขตที่บริษัทฯ ได้จดทะเบียนจัดตั้งขึ้น

1.2 คำศัพท์ใด ๆ ที่ไม่ได้กำหนดนิยามไว้ในสัญญาฉบับนี้ให้เป็นไปตามนิยามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

1.3 เอกสารแนบท้ายสัญญาฉบับนี้ถือเป็นส่วนหนึ่งของสัญญาและมีผลบังคับใช้เช่นเดียวกับสัญญา การอ้างอิงใด ๆ ถึงสัญญาฉบับนี้ให้รวมถึงเอกสารแนบท้ายสัญญาด้วย

1.4 ในกรณีที่ขัดถกกันระหว่างสัญญาฉบับนี้และสัญญาหลักขัดหรือแย้งหรือไม่ชัดเจน ให้ถือตามข้อตกลงในสัญญาฉบับนี้

2. วัตถุประสงค์ในการแบ่งปันข้อมูลและข้อมูลส่วนบุคคลที่ถูกแบ่งปัน

2.1 สัญญาฉบับนี้กำหนดขอบเขตการแบ่งปันข้อมูลส่วนบุคคลระหว่างคู่สัญญาซึ่งต่างฝ่ายต่างมีฐานะที่เป็นผู้ควบคุมข้อมูลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกำหนดสิทธิหน้าที่ระหว่างคู่สัญญาทั้งสองฝ่าย

2.2 คู่สัญญาทั้งสองเห็นว่าการแบ่งปันข้อมูลส่วนบุคคลให้แก่กันนั้นเป็นสิ่งที่จำเป็นต่อการดำเนินธุรกิจของตนเพื่อให้บรรลุวัตถุประสงค์ที่ได้ตกลงกันไว้ในสัญญาหลัก

2.3 รายละเอียดความร่วมมือทางธุรกิจระหว่างคู่สัญญา วัตถุประสงค์ที่ตกลงกัน ประเภทของข้อมูลส่วนบุคคลที่ถูกแบ่งปัน และประเภทของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องให้เป็นไปตามที่ปรากฏในเอกสารแนบท้าย 1

2.4 คู่สัญญาแต่ละฝ่ายจะประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันตามวัตถุประสงค์ที่ได้ตกลงกันเท่านั้น และจะไม่ประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันกันนอกเหนือจากวัตถุประสงค์ที่ได้ตกลงกัน เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากคู่สัญญาอีกฝ่าย

2.5 ข้อมูลส่วนบุคคลที่แบ่งปันกันจะต้องเป็นข้อมูลซึ่งเกี่ยวข้องหรือจำเป็นสำหรับวัตถุประสงค์ที่ได้ตกลงกัน

2.6 [คู่สัญญาแต่ละฝ่ายจะแต่งตั้งบุคคลหนึ่งขึ้นเป็นบุคคลติดต่อหลัก สำหรับการดำเนินการตามสัญญานี้ รวมถึงกรณีมีประเด็นปัญหาใด ๆ เกิดขึ้นจากการแบ่งปันข้อมูลระหว่างกัน]

3. การประมวลผลโดยชอบด้วยกฎหมาย

3.1 คู่สัญญาแต่ละฝ่ายจะปฏิบัติหน้าที่ของตนในฐานะผู้ควบคุมข้อมูลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล และจะประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันตามสัญญาฉบับนี้และกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎ ระเบียบ ประกาศ และคำสั่งที่มีผลใช้บังคับตลอดระยะเวลาของสัญญาฉบับนี้ โดยคู่สัญญาแต่ละฝ่ายจะต้องประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันโดยมีฐานทางกฎหมายรองรับ

3.2 สำหรับข้อมูลส่วนบุคคลที่ถูกแบ่งปัน ผู้เปิดเผยข้อมูลจะต้องแจ้งข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล และข้อมูลอื่นใดที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

3.4 ผู้รับข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล และข้อมูลอื่นใดที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

4. **การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น – กรณีที่มีการโอนข้อมูลไปต่างประเทศ**
 - 4.1 นอกเหนือจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย บริษัทฯ จะต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับในประเทศของตนตลอดระยะเวลาของสัญญาฉบับนี้
 - 4.2 ในกรณีที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับในประเทศอื่นข้างต้นมีความขัดแย้งกัน ให้ใช้กฎหมายของประเทศซึ่งมีความเคร่งครัดกว่าได้เฉพาะเท่าที่ไม่ขัดต่อกฎหมายของประเทศไทย
5. **สิทธิของเจ้าของข้อมูล**
 - 5.1 ผู้สัญญาแต่ละฝ่ายตกลงที่จะให้ความช่วยเหลือตามสมควรตามที่ผู้สัญญาอีกฝ่ายร้องขอ เพื่อให้ผู้สัญญาอีกฝ่ายหนึ่งสามารถดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ภายในระยะเวลาที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด
 - 5.2 ผู้สัญญาแต่ละฝ่ายมีหน้าที่ในการจัดทำและเก็บรักษาบันทึกคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และการดำเนินการใด ๆ ที่ได้กระทำเพื่อตอบสนองคำร้องขอใช้สิทธิดังกล่าว
6. **การจัดเก็บและการลบข้อมูลส่วนบุคคล**
 - 6.1 ผู้รับข้อมูลจะเก็บหรือประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันเป็นระยะเวลาเท่าที่จำเป็นเพื่อดำเนินการตามวัตถุประสงค์ที่ได้ตกลงกันไว้ หรือเพื่อปฏิบัติตามระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามกฎหมาย
 - 6.2 ผู้รับข้อมูลจะต้องดำเนินการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลที่ถูกแบ่งปัน ในกรณีดังต่อไปนี้
 - (ก) เมื่อสัญญาฉบับนี้ครบกำหนดอายุสัญญาหรือสิ้นสุดลงด้วยเหตุอื่น
 - (ข) เมื่อผู้สัญญาหมกความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันกัน
7. **การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ**

ผู้รับข้อมูลจะไม่ส่งหรือโอนข้อมูลส่วนบุคคลที่ถูกแบ่งปันไปยังบุคคลภายนอกที่อยู่นอกประเทศไทย เว้นแต่การโอนดังกล่าวเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และผู้รับข้อมูลได้แจ้งให้ผู้เปิดเผยข้อมูลทราบล่วงหน้าเป็นลายลักษณ์อักษรแล้ว ทั้งนี้ การโอนข้อมูลส่วนบุคคลที่ถูกแบ่งปันนี้ให้รวมถึงการจ้างช่วงสำหรับการประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันและการให้บุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลที่ถูกแบ่งปันด้วย
8. **การรักษาความมั่นคงปลอดภัย**
 - 8.1 ผู้เปิดเผยข้อมูลจะต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัยในการส่งข้อมูลส่วนบุคคลที่ถูกแบ่งปันให้แก่ผู้รับข้อมูลโดยการใช้วิธีการที่เหมาะสม
 - 8.2 ผู้สัญญาทั้งสองฝ่ายตกลงจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล รวมถึงปฏิบัติตามกฎหมายที่เกี่ยวข้องด้วย
9. **การรั่วไหลของข้อมูลส่วนบุคคล และกระบวนการรายงาน**
 - 9.1 ผู้สัญญาแต่ละฝ่ายมีหน้าที่ในการรายงานการรั่วไหลของข้อมูลส่วนบุคคลที่เกิดขึ้นจากฝ่ายของตนต่อหน่วยงานกำกับดูแลและ/หรือเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ และจะต้องแจ้งให้ผู้สัญญาอีกฝ่ายหนึ่งทราบถึงการรั่วไหลของข้อมูลส่วนบุคคลนั้นโดยทันทีในทุกกรณี
 - 9.2 ผู้สัญญาจะให้ความช่วยเหลือผู้สัญญาอีกฝ่ายหนึ่งตามความจำเป็นและตามสมควร เพื่อช่วยให้ผู้สัญญาอีกฝ่ายสามารถจัดการการรั่วไหลของข้อมูลส่วนบุคคลใด ๆ ได้อย่างรวดเร็วและเหมาะสม

10. การรับข้อพิพาท

ในกรณีที่เกิดข้อพิพาท หรือการเรียกร้องใด ๆ โดยเจ้าของข้อมูลส่วนบุคคล หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลต่อคู่สัญญาฝ่ายหนึ่งหรือทั้งสองฝ่าย คู่สัญญาจะแจ้งให้คู่สัญญาอีกฝ่ายหนึ่งทราบถึงข้อพิพาท หรือการเรียกร้องที่เกิดขึ้น และจะร่วมมือกันแก้ไขปัญหาดังกล่าวตามความเหมาะสม

11. คำรับรองและรับประกัน

11.1 คู่สัญญาแต่ละฝ่ายรับรองและรับประกันว่าจะดำเนินการดังต่อไปนี้

(ก) จะประมวลผลข้อมูลส่วนบุคคลที่ถูกแบ่งปันให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมาย กฎ ระเบียบ คำสั่ง ข้อกำหนดมาตรฐาน หรือแนวปฏิบัติอื่นใดที่ใช้บังคับกับการดำเนินการประมวลผลของคู่สัญญานั้น

(ข) ตอบข้อซักถามของหน่วยงานกำกับดูแลภายในระยะเวลาที่กำหนด

(ค) ตอบสนองต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(ง) ปฏิบัติตามขั้นตอนที่เหมาะสมเพื่อให้เป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัย

11.2 ผู้เปิดเผยข้อมูลรับรองและรับประกันว่าผู้เปิดเผยข้อมูลมีสิทธิที่จะเปิดเผยข้อมูลส่วนบุคคลที่ถูกแบ่งปันแก่ผู้รับข้อมูล และการเปิดเผยดังกล่าวเป็นไปโดยชอบด้วยกฎหมาย

12. การชดเชยค่าเสียหาย

คู่สัญญาแต่ละฝ่ายตกลงจะชดเชยค่าเสียหายให้แก่คู่สัญญาอีกฝ่ายหนึ่ง รวมถึงปกป้องคู่สัญญาอีกฝ่ายหนึ่งจากความเสียหาย การสูญหาย การเรียกร้อง ค่าเสียหาย ความรับผิดชอบ หรือค่าใช้จ่ายใด ๆ อันเนื่องมาจากการกระทำผิดสัญญาข้อใดข้อหนึ่งภายใต้สัญญานี้

13. ระยะเวลาและการสิ้นสุดสัญญา

13.1 สัญญานี้ให้มีผลใช้บังคับระหว่างคู่สัญญาตามระยะเวลาที่ระบุในเอกสารแนบท้าย 1 เว้นแต่

คู่สัญญาฝ่ายหนึ่งฝ่ายใดจะบอกเลิกสัญญาก่อนกำหนด โดยบอกกล่าวล่วงหน้าเป็นลายลักษณ์อักษรไปยังคู่สัญญาอีกฝ่ายหนึ่งไม่น้อยกว่า **[โปรดระบุระยะเวลาที่บริษัท _____ เห็นว่าเหมาะสม เช่น 30 (สามสิบ) วัน]**

13.2 การสิ้นสุดของสัญญานี้จะไม่ส่งผลกระทบต่อสิทธิใด ๆ ที่คู่สัญญาฝ่ายหนึ่งฝ่ายใดมีตามกฎหมายหรือตามสัญญานี้ต่อคู่สัญญาอีกฝ่ายหนึ่งอันเนื่องมาจากการกระทำผิดสัญญานี้

13.3 ข้อตกลงใด ๆ ภายใต้สัญญานี้ยังคงมีผลใช้บังคับต่อไปถึงแม้ว่าสัญญาหลักสิ้นสุดแล้ว

14. การบอกกล่าว

การส่งคำบอกกล่าว หรือการติดต่อสื่อสารใด ๆ ระหว่างคู่สัญญาภายใต้สัญญานี้ ต้องทำเป็นลายลักษณ์อักษรและจัดส่งไปยังบุคคลติดต่อหลักและไปยังที่อยู่ประจำตัว (หรือที่อยู่อื่นของคู่สัญญาฝ่ายหนึ่งฝ่ายใดตามที่ระบุในหนังสือบอกกล่าวซึ่งได้ส่งโดยชอบแล้วตามสัญญานี้)

บริษัท: **[ระบุบุคคลติดต่อหลัก และข้อมูลติดต่อ]**

บริษัท: **[ระบุบุคคลติดต่อหลัก และข้อมูลติดต่อ]**

15. เบ็ดเตล็ด

15.1 ค่าใช้จ่าย คู่สัญญาแต่ละฝ่ายจะเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากการปฏิบัติตามสัญญานี้ด้วยตนเอง

15.2 การเปลี่ยนแปลงแก้ไข หรือสละสิทธิ ข้อตกลงภายใต้สัญญานี้ข้อมไม่อาจแก้ไข สละสิทธิ หรือเปลี่ยนแปลงโดยประการอื่นได้ เว้นแต่คู่สัญญาทั้งสองฝ่ายจะตกลงกันเป็นลายลักษณ์อักษรและลงนามโดยผู้มีอำนาจของคู่สัญญาแต่ละฝ่าย อนึ่ง การละเลยหรือล่าช้าของคู่สัญญาฝ่ายหนึ่งในการใช้สิทธิประการใด ๆ ภายใต้สัญญานี้ไม่เป็นเหตุให้คู่สัญญาฝ่ายนั้นเสียสิทธิดังกล่าว หรือสิทธิอื่นใดภายใต้สัญญานี้

15.3 สัญญาทั้งหมด สัญญานี้ก่อให้เกิดความตกลงและความเข้าใจทั้งหมดระหว่างคู่สัญญาทั้งสองฝ่าย และมีผลบังคับใช้แทนความตกลงและความเข้าใจก่อนหน้านี้โดยสิ้นเชิง (ถ้ามี) ระหว่างคู่สัญญา

15.4 การเป็นโมฆะบางส่วน ข้อตกลงใด ๆ ของสัญญานี้ ซึ่งเป็นโมฆะหรือไม่สามารถบังคับใช้ได้ ให้มีผลเป็นโมฆะหรือไม่สามารถบังคับใช้ได้เฉพาะข้อตกลงดังกล่าวเท่านั้น และมีผลทำให้ข้อตกลงอื่นใดในสัญญานี้ตกเป็นโมฆะหรือไม่สามารถบังคับใช้ได้

15.5 กฎหมายที่บังคับและเขตอำนาจศาล สัญญานี้มีขึ้นอยู่ภายใต้บังคับของกฎหมายไทย คู่สัญญาตกลงที่จะเสนอข้อพิพาทต่อศาลที่มีเขตอำนาจในประเทศไทยเพื่อระงับข้อพิพาทใด ๆ ที่เกิดจาก หรือเกี่ยวกับสัญญานี้

[ส่วนที่เหลือของหน้านี้เว้นว่างไว้โดยเจตนา]

เพื่อเป็นหลักฐานแห่งการนี้ สัญญาฉบับนี้ได้ทำขึ้นเป็นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาทั้งสองฝ่ายได้อ่านและเข้าใจข้อความในสัญญาโดยตลอดแล้ว จึงได้ลงลายมือชื่อและประทับตราสำคัญ (ถ้ามี) ณ วันเดือนปีที่ปรากฏข้างต้น

บริษัท _____ จำกัด (มหาชน)

[ชื่อบริษัทฯ]

ลงชื่อ _____

ชื่อ: [□]

ตำแหน่ง: [□]

[ตราประทับบริษัท]

[ตราประทับบริษัท]

พยาน

พยาน

ลงชื่อ _____

ชื่อ: [□]

ลงชื่อ _____

ชื่อ: [□]

เอกสารแนบท้าย 1
รายละเอียดการแบ่งปันข้อมูล

การจัดการธุรกิจระหว่างคู่สัญญา	[ระบุการดำเนินธุรกิจระหว่างคู่สัญญาซึ่งมีความจำเป็นต่อการแบ่งปันข้อมูล]
วัตถุประสงค์ที่ตกลงกัน	[ระบุวัตถุประสงค์สำหรับการแบ่งปันข้อมูลส่วนบุคคล]
ประเภทของข้อมูลที่ถูกแบ่งปัน	[ระบุประเภทของข้อมูลที่เกี่ยวข้อง ยกตัวอย่างเช่น ประเภทของข้อมูลส่วนบุคคลดังต่อไปนี้ อาจถูกแบ่งปันระหว่างคู่สัญญาตามระหว่างระยะเวลาตามสัญญา - ข้อมูลซึ่งระบุถึงตัวตนและช่องทางการติดต่อ ได้แก่ (ชื่อ เบอร์โทรศัพท์ และอีเมล)]
ประเภทของเจ้าของข้อมูล	[ระบุบุคคลที่เกี่ยวข้องกับข้อมูล]
ระยะเวลาของสัญญาแบ่งปันข้อมูล	[ระบุระยะเวลาซึ่งสัญญาแบ่งปันข้อมูลนี้จะมีผลใช้บังคับ]

4. ตัวอย่าง แบบฟอร์มคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

แบบฟอร์มคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

เพื่อตอบสนองต่อคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ระยะเวลาการดำเนินการตามสิทธิคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

ข้อที่	สิทธิของคำร้อง	ระยะเวลาดำเนินการให้แล้วเสร็จ
1	สิทธิในการเข้าถึงข้อมูลส่วนบุคคล	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล ¹
2	สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล
3	สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล
4	สิทธิในการลบข้อมูลส่วนบุคคล ซึ่งรวมถึงกรณีเจ้าของข้อมูลเพิกถอนความยินยอม ²	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล
5	สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล ซึ่งรวมถึงกรณีเจ้าของข้อมูลเพิกถอนความยินยอม ³	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล
6	สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล	30 วันนับแต่วันที่ได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างเอกสารและแบบฟอร์มที่เกี่ยวข้อง

หัวข้อ	เลขที่อ้างอิง
แบบฟอร์มที่เกี่ยวข้อง	1
• แบบฟอร์มคำร้องของเจ้าของข้อมูลส่วนบุคคล	1.1
• ทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล	1.2
• หนังสือแจ้งการปฏิเสธคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล	1.3
• หนังสือแจ้งยืนยันเพื่อการดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคล	1.4

¹ อ้างอิงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 ว่าด้วยการกำหนดการดำเนินการแล้วเสร็จสำหรับคำร้องตามสิทธิการขอเข้าถึงข้อมูลส่วนบุคคล

² สำหรับกรณีเพิกถอนความยินยอม หน่วยงานที่เกี่ยวข้องจำเป็นต้องพิจารณาดำเนินการลบข้อมูลส่วนบุคคลทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ดำเนินการเพิกถอนความยินยอมแล้ว หากไม่มีความจำเป็นหรือไม่มีฐานกฎหมายอื่นๆ ที่จะประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป

³ สำหรับกรณีถอนความยินยอม หน่วยงานที่เกี่ยวข้องจำเป็นต้องพิจารณาการระงับการประมวลผลหรือลบข้อมูลส่วนบุคคลทั้งหมดออกจากระบบของบริษัท เว้นแต่ มีเหตุให้สามารถดำเนินการประมวลผลได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่น การประมวลผลเนื่องจากการปฏิบัติตามสัญญาระหว่างบริษัทและเจ้าของข้อมูลส่วนบุคคล หรือเพื่อปกป้องสิทธิในชีวิตของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

1.1 แบบฟอร์มคำร้องของเจ้าของข้อมูลส่วนบุคคล

แบบฟอร์มการขอใช้สิทธิของเจ้าของข้อมูล

1. รายละเอียดเบื้องต้นเกี่ยวกับผู้ขอ

ชื่อ นามสกุล:	
หมายเลขโทรศัพท์/อีเมล:	
[โปรดระบุรายละเอียดอื่นๆ (ถ้ามี)]:	

2. รายละเอียดเบื้องต้นเกี่ยวกับเจ้าของข้อมูล (ไม่ต้องกรอกส่วนนี้กรณีเจ้าของข้อมูลเป็นบุคคลเดียวกับผู้ขอ)

ชื่อ นามสกุล:	
หมายเลขโทรศัพท์/อีเมล:	
[โปรดระบุรายละเอียดอื่นๆ (ถ้ามี)]:	

3. รายละเอียดของการขอใช้สิทธิ

3.1 ประเภทข้อมูลส่วนบุคคลที่ประสงค์จะใช้สิทธิ

--

3.2 ประเภทการขอใช้สิทธิ

- ขอลอนความยินยอม
- ขอเข้าถึงและ/หรือขอรับสำเนาข้อมูลส่วนบุคคล
- ขอให้เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูล
- ขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
- ขอให้โอนย้ายข้อมูลส่วนบุคคล
- ขอให้ลบ ทำลายหรือทำให้ไม่สามารถระบุตัวเจ้าของข้อมูลได้

- ขอให้ระงับการใช้ข้อมูลส่วนบุคคล
- ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล

3.3 รายละเอียดการขอใช้สิทธิและเหตุผลในการขอ

■ หลักฐานประกอบ

[หลักฐานการยืนยันตัวตน เช่น]

- กรณีสัญชาติไทย สำเนาบัตรประชาชนของเจ้าของข้อมูล และ / หรือตัวแทน (ถ้ามี) (โปรดลบข้อมูลศาสนาและกรุ๊ปเลือดออกก่อนนำส่งบริษัท (ถ้ามี))
- กรณีต่างชาติ สำเนาหนังสือเดินทางเจ้าของข้อมูลและ/หรือตัวแทน (ถ้ามี)
- หนังสือมอบอำนาจ (กรณีผู้ขอเป็นตัวแทนของเจ้าของข้อมูล)
- [หลักฐานอื่นๆ โปรดระบุ] _____

[หลักฐานประกอบคำขอใช้สิทธิ เช่น เอกสารประกอบการเปลี่ยนแปลงหรือแก้ไขข้อมูลส่วนบุคคล เป็นต้น]

- [โปรดระบุ] _____

■ การรับทราบและรับรอง

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้นเป็นความจริงและถูกต้อง รวมถึงรับทราบว่าบริษัทอาจติดต่อข้าพเจ้าที่รายละเอียดการติดต่อที่ให้ไว้ข้างต้นเพื่อสอบถามข้อมูลเพิ่มเติมเพื่อให้การดำเนินการตามคำขอของข้าพเจ้าเป็นไปอย่างถูกต้องครบถ้วน และบริษัทสงวนสิทธิที่จะปฏิเสธคำขอของข้าพเจ้าในบางกรณีที่กฎหมายกำหนดหรือกรณีที่ข้าพเจ้าไม่สามารถแสดงหลักฐานประกอบคำขอให้แก่บริษัทได้ (ถ้ามี)

ลายมือชื่อผู้ขอ:	
วัน เดือน ปี (พ.ศ.)	

1.2 ทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล (ส่วนที่ 1)

ทะเบียนคุมคำร้องของเจ้าของข้อมูลส่วนบุคคล (DSR Log Register)												
ข้อมูลเปิดสถานะ (Open Ticket) ของคำร้องขอใช้สิทธิของเจ้าของข้อมูล												
ลำดับที่	ข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล (Data Subject Information)					ข้อมูลที่เกี่ยวข้องกับผู้บันทึกคำร้อง (In-Charge of Open Ticket)				รายละเอียดคำร้องของเจ้าของข้อมูลส่วนบุคคล		
	ชื่อ-นามสกุล เจ้าของข้อมูล	ประเภท เจ้าของข้อมูล (Data Subject) (1)	ประเภท เจ้าของข้อมูล (โปรดระบุ)	ข้อมูลเพื่อการ ติดต่อกลับ	สามารถระบุ ตัวตนได้หรือไม่	ชื่อ-นามสกุล	Business Unit (กลุ่มธุรกิจ / กลุ่ม งาน)	Department (ฝ่าย)	Division (ส่วน)	วันที่ร้องขอ (ว/ด/ป)	ประเภทคำ ร้อง	รายละเอียดคำร้อง
1	นาย xx xxxx	ลูกค้าปัจจุบัน	-	abc@gmail.com	ได้	นาย xx xxxx	xxxx	xxx	-	xx/xx/xxxx	การระงับใช้ ข้อมูลส่วน บุคคล	ระงับการใช้อีเมลในการ ประชาสัมพันธ์ Promotion ต่าง ๆ

หมายเหตุ:

- (1) บริษัทสามารถแบ่งประเภทประเภทของเจ้าของข้อมูลได้ ดังนี้
- ลูกค้าที่มุ่งหวัง
 - ลูกค้าปัจจุบัน
 - ผู้ขาย
 - พนักงานปัจจุบัน
 - พนักงานเก่า
 - ผู้สมัครเข้าทำงาน
 - อื่นๆ (โปรดระบุ)

1.3 หนังสือแจ้งการปฏิเสธคำร้องตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

หนังสือแจ้งการปฏิเสธคำร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัท _____ จำกัด ขอเรียนแจ้งผลการพิจารณาเบื้องต้นเกี่ยวกับคำร้องของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล บริษัทได้พิจารณาแบบฟอร์มคำร้อง ณ วันที่ _____ แล้ว บริษัทต้องขอภัยเป็นอย่างสูงที่ไม่สามารถอนุมัติให้ดำเนินการตามคำร้องดังกล่าวได้ เนื่องจากเป็นไปตามเงื่อนไขการปฏิเสธคำร้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล

กรณีที่การประมวลผลนั้นเป็นการดำเนินการตามหน้าที่ที่เกี่ยวกับประโยชน์สาธารณะ

กรณีที่การดำเนินการดังกล่าวส่งผลกระทบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ

กรณีเป็นการเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ เพื่อปฏิบัติตามกฎหมาย

อื่น ๆ ระบุ:

อย่างไรก็ตาม เจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญสำหรับกรณีที่ได้รับการปฏิเสธดังกล่าว ตามที่ระบุในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากท่านมีข้อสงสัยหรือต้องการสอบถามรายละเอียดเพิ่มเติม กรุณาติดต่อหน่วยงานคุ้มครองข้อมูลส่วนบุคคล บริษัท _____ จำกัด ได้ที่เบอร์ Call Center หรือ เบอร์ _____

ขอแสดงความนับถือ

หน่วยงานคุ้มครองข้อมูลส่วนบุคคล

บริษัท _____ จำกัด

1.4 หนังสือแจ้งยืนยันเพื่อการดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคล

หนังสือแจ้งยืนยันเพื่อดำเนินการตามคำร้องของเจ้าของข้อมูล

บริษัท _____ จำกัด ขอนำส่งหนังสือแจ้งฉบับนี้ เพื่อขอยืนยันให้ดำเนินการตามคำร้องของท่าน ตามที่บริษัทได้พิจารณาแบบฟอร์มคำร้อง ณ วันที่ _____ เรื่อง _____ อย่างไรก็ตาม บริษัทขอรายงานผลกระทบที่อาจเกิดขึ้นหลังจากดำเนินการตามคำร้องดังกล่าว ดังนี้

ทั้งนี้ รบกวนยืนยันคำร้องดังกล่าว เพื่อทางบริษัทจะพิจารณาดำเนินการตามคำร้องเป็นลำดับถัดไป

- ยืนยันให้ดำเนินการตามคำร้อง พร้อมยอมรับผลกระทบจากการดำเนินการดังกล่าว
- ยกเลิกคำร้องให้ดำเนินการ

หากท่านมีข้อสงสัยหรือต้องการสอบถามรายละเอียดเพิ่มเติม กรุณาติดต่อหน่วยงานคุ้มครองข้อมูลส่วนบุคคล บริษัท _____ จำกัด ได้ที่เบอร์ Call Center หรือ เบอร์ _____

เจ้าของข้อมูลส่วนบุคคล

ขอแสดงความนับถือ
หน่วยงานคุ้มครองข้อมูลส่วนบุคคล
บริษัท _____ จำกัด