



CHECK LIST

เอกสารและแบบฟอร์ม

PDPA

ของบริษัท

รวมเอกสารและแบบฟอร์ม
ที่เกี่ยวข้องกับการ Checklist PDPA

รวบรวมโดย
สำนักพิมพ์ธรรมนิติ



CHECK LIST

เอกสารและแบบฟอร์ม

PDPA

ของบริษัท





โดย : สำนักพิมพ์ธรรมนิติ
พิมพ์ครั้งแรก : กันยายน 2565
ISBN (e-Book) : 978-616-302-248-6
จัดทำโดย : สำนักพิมพ์ธรรมนิติ
เจ้าของ : บริษัท ธรรมนิติ เพรส จำกัด
ที่ปรึกษา : ดารารัตต์ พิษมงคล
กองบรรณาธิการ : ญาภา ทวยเจริญ
พิสูจน์อักษร : จันทรจิรา ชื้อพร้อม
ประสานงาน : ทิพสุคนธ์ วงษ์เมือง
ออกแบบ-จัดรูปเล่ม : ศษามา พูลสวัสดิ์

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

Checklist เอกสารและแบบฟอร์มต่างๆ ที่เกี่ยวข้องกับ PDPA ของบริษัท.--

กรุงเทพฯ : ธรรมนิติ เพรส, 2565.

30 หน้า.

1. การป้องกันข้อมูล. 2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.
I. ชื่อเรื่อง.

342.0858

ISBN (e-Book) : 978-616-302-248-6

จัดทำโดย

บริษัท ธรรมนิติ เพรส จำกัด เลขที่ 178 อาคารธรรมนิติ ชั้น 4

ซอยเพิ่มทรัพย์ (ประชาชื่น 20) ถนนประชาชื่น แขวงบางซื่อ เขตบางซื่อ กรุงเทพฯ 10800

โทรศัพท์ (02) 555-0713 โทรสาร (02) 555-0728

ได้รับอนุญาตจัดพิมพ์จากเจ้าของลิขสิทธิ์ถูกต้องตามกฎหมาย สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 (ห้ามคัดลอกหรือถ่ายสำเนาส่วนหนึ่งส่วนใดของหนังสือเล่มนี้ โดยไม่ได้รับอนุญาต มิฉะนั้นจะถือว่ามีความผิดตามกฎหมาย)



ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายในองค์กร ต้องกระทำภายใต้ฐานทางกฎหมายที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งต้องอธิบายรายละเอียดที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่บุคลากรและพนักงานของบริษัทหรือบุคคลภายนอกที่เป็นผู้กระทำการแทนในนามของบริษัท

หนังสือเล่มนี้เป็นการรวบรวมรายการตรวจสอบกระบวนการดำเนินงานของส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล อาทิ ฝ่ายนโยบาย และยุทธศาสตร์ ฝ่ายเทคโนโลยีสารสนเทศ และหน่วยงานที่ทำหน้าที่เก็บรวบรวม ใช้ข้อมูล และแบบฟอร์มบันทึกข้อตกลงเพิ่มเติมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้แต่ละองค์กรนำไปใช้ตรวจสอบว่าหากจะดำเนินการภายใต้หลักกฎหมาย PDPA ให้ครบถ้วนจะต้องดำเนินการอย่างไร



• Checklist เอกสารและแบบฟอร์มต่างๆ ที่เกี่ยวข้องกับ PDPA ของบริษัท	06
• Checklist แนวทางการคุ้มครองข้อมูลส่วนบุคคล สำหรับฝ่ายนโยบายและยุทธศาสตร์	08
• Checklist แนวทางการคุ้มครองข้อมูลส่วนบุคคล สำหรับฝ่ายเทคโนโลยีสารสนเทศ	17
• Checklist แนวทางการคุ้มครองข้อมูลส่วนบุคคล สำหรับหน่วยงานที่เก็บรวบรวม ใช้ข้อมูล	22
• แบบฟอร์มบันทึกข้อตกลงเพิ่มเติมการคุ้มครองข้อมูลส่วนบุคคล	27



CHECK LIST

เอกสารและแบบฟอร์มต่างๆ
ที่เกี่ยวข้องกับ PDPA ของบริษัท

รายการ		สถานะ		หมายเหตุ
1	บันทึกกิจกรรมการประมวลข้อมูลส่วนบุคคล (Record of Process)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
2	ประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
3	ประกาศความเป็นส่วนตัว (Privacy Notice)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
4	แบบคำร้องขอใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคล (Data Subject Request Form)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
5	บันทึกข้อตกลงเพิ่มเติมการคุ้มครองข้อมูล ส่วนบุคคล (Data Processing Agreement)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
6	แบบฟอร์มบันทึกการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
7	หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูล	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	
8	แบนเนอร์ขอความยินยอมการใช้คุกกี้ (Cookie Consent Banner) กรณีบริษัทมีเว็บไซต์/ ช่องทางออนไลน์	ดำเนินการแล้ว ☐	ประกาศใช้แล้ว ☐	

* กรณีที่ PDPA มีกฎหมายลำดับรองหรือประกาศหลักเกณฑ์และแบบปฏิบัติเพิ่มเติมที่ชัดเจนขึ้นเกี่ยวกับนิยามของผู้ที่เกี่ยวข้องต่างๆ ตลอดจนบทบาทหน้าที่วิธีการแต่งตั้ง
จะพิจารณาปรับปรุงตามความเหมาะสมอีกครั้ง



CHECK LIST

แนวทางการคุ้มครองข้อมูลส่วนบุคคล
สำหรับฝ่ายนโยบายและยุทธศาสตร์

1. การกำหนดนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคล ของลูกค้าหรือผู้ใช้บริการ

รายการ		สถานะ		หมายเหตุ
1	จำแนกความสำคัญของข้อมูลตามลักษณะของข้อมูล	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
2	กำหนดมาตรการการรักษาความปลอดภัยตามระดับความสำคัญของข้อมูลที่จำแนก	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
3	จัดให้มี Data Privacy Policy ที่ชัดเจน	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
4	กำหนดระดับของการเข้าถึงข้อมูลไว้ใน Access Control Policy	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
5	กำหนดการลบหรือทำลายข้อมูล	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

2. การกำหนดมาตรการทางเทคนิคที่จำเป็นสำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ

รายการ		สถานะ		หมายเหตุ
1	กำหนดให้มี Access Authorization System	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
2	กำหนดแนวปฏิบัติให้ลูกค้าแจ้งข้อมูล/รายละเอียดที่สามารถระบุและยืนยันตัวตนของลูกค้า	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
3	จัดให้มีการตรวจสอบการเข้าถึงข้อมูลของลูกค้าเป็นระยะๆ อย่างสม่ำเสมอ	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
4	กำหนดวิธีการเข้าถึงข้อมูลในระบบคอมพิวเตอร์ผ่านทางเครือข่ายคอมพิวเตอร์ (กรณีมีหน่วยงานสาขา)	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
5	กำหนดมาตรการหรือวิธีการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้า/ผู้ใช้บริการที่เกี่ยวข้องกับการใช้ Internet	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
6	จัดให้มีวิธีการป้องกันการเข้าถึง/เปิดเผยข้อมูลต่างๆ ของลูกค้าที่จัดเก็บอยู่ในรูปของเอกสาร	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
7	กำหนดวิธีการจัดเก็บสำเนาเอกสารแสดงตนหรือยืนยันตัวตนบุคคล	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

3. การรักษาความปลอดภัยของสถานที่และอุปกรณ์

รายการ		สถานะ		หมายเหตุ
1	จัดให้มีการควบคุมดูแลการเข้าถึงสถานที่ตั้งของระบบคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย สถานที่เก็บเอกสาร	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
2	กำหนดวิธีการติดตั้งเครื่องแฟกซ์	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

4. ข้อกำหนดของพนักงานที่มีหน้าที่รับผิดชอบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

รายการ		สถานะ		หมายเหตุ
1	จัดให้มีการฝึกอบรมอย่างสม่ำเสมอ	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
2	กำหนดวิธีการรับพนักงานใหม่ (ตำแหน่งที่สามารถเข้าถึงข้อมูลที่สำคัญของลูกค้า)	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
3	จัดให้มีการกำกับ ตรวจสอบ เฝ้าระวังการปฏิบัติงานของพนักงาน	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

5. การโอนข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ

รายการ		สถานะ		หมายเหตุ
1	กำหนดวิธีการที่เหมาะสม หากมีการมอบหมาย/จ้างบุคคลที่สามทำหน้าที่ในการให้บริการ/ซ่อมแซม/บำรุงรักษา	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

6. การทบทวนและประเมินระบบและมาตรการการรักษาความปลอดภัยที่มีอยู่

รายการ		สถานะ		หมายเหตุ
1	กรณีสภาพแวดล้อมของการทำธุรกิจ/เทคโนโลยีที่เปลี่ยนแปลงไป	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	
2	กรณีมีการละเมิดข้อมูลส่วนบุคคล	ดำเนินการแล้ว ☐	อยู่ระหว่างดำเนินการ ☐	

* รายละเอียดเพิ่มเติมตามเอกสารแนบท้าย

* กรณีที่ PDPA มีกฎหมายลูกหรือประกาศหลักเกณฑ์และแนวปฏิบัติเพิ่มเติมที่ชัดเจนขึ้นเกี่ยวกับนิยามของผู้เกี่ยวข้องต่างๆ ตลอดจนบทบาทหน้าที่ วิธีการแต่งตั้ง จะพิจารณาปรับปรุงตามความเหมาะสมอีกครั้ง

ผู้ตรวจ..... วันที่.....