



แบบแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

(Personal Data Breach Report Form)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า ภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ดังนั้น เพื่อให้ทางเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถดำเนินการตามบทบัญญัติดังกล่าว โปรดระบุและแจ้งรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลเท่าที่ท่านสามารถระบุได้ เพื่อให้ทางบริษัทฯ ตรวจสอบและแจ้งผลต่อไป

โดยท่านสามารถระบุรายละเอียดเหตุละเมิดข้อมูลส่วนบุคคลเท่าที่ท่านสามารถระบุได้ ตามแบบฟอร์มต่อไปนี้ และยื่นแบบร้องเรียนนี้ด้วยตนเอง หรือโดยการมอบอำนาจมาที่ บริษัทฯ หรือนำส่งโดยทางจดหมายอิเล็กทรอนิกส์ (e-mail) : compliancerm@prospectrm.com ทั้งนี้ ภายในระยะเวลาสี่สิบสองชั่วโมงนับแต่ทราบเหตุละเมิดดังกล่าว

รายละเอียดผู้แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ชื่อ-นามสกุล _____
หมายเลขโทรศัพท์ติดต่อ _____
ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail) _____
ที่อยู่เพื่อการติดต่อ _____

พบเหตุละเมิด และเป็นเจ้าของข้อมูลส่วนบุคคลแจ้งเหตุด้วยตัวเอง

แจ้งเหตุละเมิดข้อมูลส่วนบุคคลโดยตัวแทน (แนบเอกสารประกอบการมอบอำนาจ¹)

บริษัทฯ ขอสงวนสิทธิในการสอบถามข้อมูล หรือเรียกเอกสารเพิ่มเติมจากผู้แจ้งเหตุละเมิดข้อมูลส่วนบุคคล หากข้อมูลที่ได้รับไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่า ผู้ยื่นแบบเป็นเจ้าของข้อมูลหรือมีอำนาจในการยื่นแบบดังกล่าว บริษัทฯ ขอสงวนสิทธิในการปฏิเสธการดำเนินการต่อคำร้อง และ/หรือการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของท่าน

รายละเอียดเหตุละเมิดข้อมูลส่วนบุคคล

1. วันและเวลาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล วันที่ _____ เวลา _____
2. วันและเวลาที่พบการเหตุละเมิดข้อมูลส่วนบุคคล วันที่ _____ เวลา _____
3. วันและเวลาเริ่มต้นของเหตุละเมิดข้อมูลส่วนบุคคล วันที่ _____ เวลา _____

ลายมือชื่อผู้แจ้งเหตุ : _____ วันที่ : _____

¹ ชุดเอกสารการมอบอำนาจ ประกอบด้วย 1) หนังสือมอบอำนาจที่ลงนามแล้ว พร้อมติดอากรแสตมป์ 2) สำเนาเอกสารแสดงตนที่ออกให้โดยหน่วยงานราชการที่ยังไม่หมดอายุของผู้มอบอำนาจ เช่น สำเนาบัตรประจำตัวประชาชนหรือสำเนาหนังสือเดินทาง

4. ลักษณะเหตุละเมิดข้อมูลส่วนบุคคล (โปรดอธิบาย เช่น การโจรกรรมข้อมูลส่วนบุคคล/การเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต/การจัดส่งข้อมูลต่อบุคคลอื่นที่ไม่มีสิทธิรับข้อมูล/อุปกรณ์อิเล็กทรอนิกส์ที่บรรจุข้อมูลส่วนบุคคลสูญหาย/การแก้ไขข้อมูลโดยไม่ได้รับความยินยอม)

5. สถานที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล (โปรดอธิบาย เช่น ภายในฝ่ายงาน / หน้าสำนักงาน)

6. ประเภทของเจ้าของข้อมูล (โปรดเลือก)

- | | |
|---|---|
| <input type="checkbox"/> ผู้ถือหน่วยทรัสต์ และบุคคลเกี่ยวข้อง | <input type="checkbox"/> กรรมการ และผู้บริหารของบริษัทฯ |
| <input type="checkbox"/> คู่ค้า ผู้เช่า และบุคคลที่เกี่ยวข้อง | <input type="checkbox"/> พนักงานของบริษัทฯ |
| <input type="checkbox"/> ที่ปรึกษา และบุคคลที่เกี่ยวข้อง | <input type="checkbox"/> บุคคลภายนอก |
| <input type="checkbox"/> ลูกจ้างตามสัญญาจ้าง หรือผู้ที่ทำงาน หรือปฏิบัติงานให้บริษัทฯ | <input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้ |

7. ประมาณการจำนวนผู้เสียหาย (โปรดเลือก)

- | | | | |
|---|-------------------------------------|--------------------------------------|---|
| <input type="checkbox"/> 1 – 9 คน | <input type="checkbox"/> 10 – 50 คน | <input type="checkbox"/> 51 – 100 คน | <input type="checkbox"/> อย่างน้อย 100 คน |
| <input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้ | | | |

8. ประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด (โปรดเลือก)

- | | |
|--|--|
| <input type="checkbox"/> ข้อมูลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล วัน/เดือน/ปีเกิด การศึกษา ข้อมูลการถือหุ้น-กรรมการ | <input type="checkbox"/> ข้อมูลอ่อนไหว เช่น เชื้อชาติ หมูโลหิต ข้อมูลสุขภาพ ประวัติอาชญากรรม ข้อมูลทางชีวภาพ ความชอบทางเพศ |
| <input type="checkbox"/> เอกสารราชการ เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง ใบขับขี่ บัตรข้าราชการ | <input type="checkbox"/> เอกสารที่ออกโดยเอกชน เช่น บัตรประจำตัวพนักงาน บัตรสมาชิก บัตรเครดิต นามบัตร |
| <input type="checkbox"/> ข้อมูลทางการเงิน | <input type="checkbox"/> ข้อมูลครอบครัวของผู้ให้ข้อมูล |
| <input type="checkbox"/> ข้อมูลอื่นๆ (โปรดระบุ) | |
| <input type="checkbox"/> ไม่สามารถระบุได้ในขณะนี้ | |

ลายมือชื่อผู้แจ้งเหตุ : _____ วันที่ : _____

9. คุณทราบเหตุละเมิดได้อย่างไร (โปรดอธิบาย เช่น ได้รับแจ้งจากเจ้าของข้อมูลถึงการละเมิด / พบการเข้าถึงระบบใน Log File ว่าถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ / ทำอุปกรณ์สูญหาย)

10. รายละเอียดโดยสรุปของเหตุละเมิด (โปรดอธิบาย เพื่อขยายความลักษณะเหตุละเมิด เพื่อให้เข้าใจเนื้อหาของการละเมิดข้อมูลส่วนบุคคล โดยอธิบายเนื้อหาเท่าที่สามารถระบุได้ รวมไปถึงคำขยายความประเภทข้อมูลที่ทราบโดยละเอียด)

11. รายละเอียดระบบเทคโนโลยีสารสนเทศและอุปกรณ์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (ถ้ามี เช่น มือถือส่วนบุคคล รวมถึงอธิบายถึงการรักษาความปลอดภัยของข้อมูลในระบบดังกล่าวโดยสรุป เช่น มีการเข้ารหัสข้อมูล หรือมีการสำรองไฟล์ไว้ในระบบของบริษัทฯ)

12. อธิบายความเสี่ยงต่อข้อมูลส่วนบุคคล (โปรดอธิบาย เช่น ผู้พบเห็นอาจสามารถเข้าถึงข้อมูลดังกล่าว และสามารถแก้ไขข้อมูลดังกล่าวโดยมิชอบ)

ลายมือชื่อผู้แจ้งเหตุ : _____ วันที่ : _____

13. ประมาณการความเสี่ยงต่อเจ้าของข้อมูล (โปรดพิจารณาเกณฑ์ความเสี่ยงตามที่ระบุในหมายเหตุของเอกสารฉบับนี้)

- ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงน้อย ไม่มีความเสี่ยง
 ไม่สามารถระบุได้ในขณะนี้

14. รายละเอียดการกระทำที่ได้ดำเนินการเพื่อเยียวยาการละเมิด (โปรดระบุมาตรการการแก้ไขปัญหา เช่น ดำเนินการ เปลี่ยนรหัสความปลอดภัย ดำเนินการค้นหาตามสถานที่ที่คาดว่าอุปกรณ์จะสูญหาย เป็นต้น)

สาเหตุของปัญหา _____

การแก้ไขระยะสั้น _____

การแก้ไขระยะยาว _____

แผนงาน และการป้องกัน การเกิดเหตุการณ์ซ้ำ _____

หน่วยงานที่รับผิดชอบในการดำเนินการตามแผนข้างต้น _____

15. การแจ้งเหตุละเมิดต่อเจ้าของข้อมูล

- ดำเนินการแจ้งเจ้าของข้อมูลเรียบร้อยแล้ว อยู่ระหว่างดำเนินการแจ้งเจ้าของข้อมูล
 อยู่ระหว่างพิจารณาว่าจะแจ้งเจ้าของข้อมูลหรือไม่ พิจารณาไม่ดำเนินการแจ้งเจ้าของข้อมูล

อนึ่ง ในกรณีที่บริษัทฯ ปฏิเสธไม่ดำเนินการตามคำร้องขอของท่าน ท่านสามารถร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หมายเลขโทรศัพท์ 02-142-1033 หรืออีเมล: pdpc@mdes.go.th

การรับทราบและยินยอม

ท่านได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่าง ๆ ที่ได้แจ้งให้แก่บริษัทฯ ทรานั้นเป็นความจริง ถูกต้อง ท่านเข้าใจดีว่าการตรวจสอบเพื่อยืนยันอำนาจ ตัวตน และถิ่นที่อยู่เป็นการจำเป็นอย่างยิ่ง เพื่อพิจารณาดำเนินการตามสิทธิที่ท่านร้องขอ หากท่านให้ข้อมูลที่ผิดพลาดด้วยเจตนาทุจริตท่านอาจถูกดำเนินคดีตามกฎหมายได้ และบริษัทฯ อาจขอข้อมูลเพิ่มเติมจากท่านเพื่อการตรวจสอบดังกล่าวเพื่อให้การดำเนินการตามคำร้องขอของท่าน อย่างถูกต้องครบถ้วนต่อไป

ในการนี้ ท่านจึงได้ลงนามไว้ เพื่อเป็นหลักฐาน

ลายมือชื่อผู้แจ้งเหตุ : _____ วันที่ : _____

สำหรับเจ้าหน้าที่เท่านั้น

สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

วันที่ได้รับแจ้งเหตุ	:	_____
วันที่บันทึกในระบบ	:	_____
ผลการพิจารณาการแจ้งเหตุ	:	_____
<input type="checkbox"/> ดำเนินการตามคำร้อง	วันที่ดำเนินการในระบบ	_____
	ดำเนินการโดย	_____
<input type="checkbox"/> ปฏิเสธคำร้อง		
เหตุผลในการปฏิเสธ (ถ้ามี)	:	_____
บันทึกในระบบโดย	:	_____ วันที่ _____
เลขที่หนังสือตอบกลับ	:	_____ วันที่ _____
ค่าธรรมเนียม (ถ้ามี)	:	_____
วันที่ได้รับชำระค่าธรรมเนียม	:	_____

ผลกระทบที่เกิดขึ้น หรือ อาจจะเกิดขึ้น จากเหตุการณ์ข้างต้น

เหตุการณ์ที่เกิดขึ้นเกี่ยวข้องกับ การควบคุมข้อมูล ประมวลผลข้อมูล การเก็บรวบรวม การ ใช่ ไม่ใช่
ใช้ การเข้าถึง การเปิดเผย การแก้ไขเปลี่ยนแปลง และ/หรือ เปิดเผยข้อมูลส่วนบุคคลโดย
ไม่ได้รับอนุญาตหรือไม่เหมาะสมหรือไม่

เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อเจ้าของข้อมูลหรือไม่ ใช่ ไม่ใช่

การแจ้งเหตุต่อหน่วยงานที่เกี่ยวข้อง

- แจ้งต่อผู้คุ้มครองข้อมูลส่วนบุคคลของบริษัท แจ้งเรียบร้อยแล้ว ยังไม่แจ้ง
- แจ้งต่อผู้บริหารสูงสุดของบริษัท แจ้งเรียบร้อยแล้ว ยังไม่แจ้ง
- แจ้งความ / ลงบันทึกประจำวันต่อเจ้าหน้าที่ตำรวจ แจ้งเรียบร้อยแล้ว ยังไม่แจ้ง
- แจ้งต่อเจ้าของข้อมูลส่วนบุคคล* มีการแจ้งเจ้าของข้อมูลเรียบร้อยแล้ว วันที่/เวลา _____
 อยู่ระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล
 บริษัทฯ และ/หรือ กองทรัสต์ฯ ตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล
 อยู่ระหว่างการพิจารณาของ บริษัทฯ และ/หรือ กองทรัสต์ฯ
 อื่นๆ (โปรดระบุ) _____
- แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล* แจ้งเรียบร้อยแล้ว วันที่/เวลา _____ ยังไม่แจ้ง
(หน่วยงานของรัฐ ที่จัดตั้งขึ้นตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

* หมายเหตุ หากเป็นกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง

การพิจารณาปัจจัยความเสี่ยง เพื่อคำนวณคะแนนสำหรับระดับความเสี่ยงตามเกณฑ์ดังต่อไปนี้

คะแนนสำหรับระดับความเสี่ยง	ระดับความเสี่ยง
0	ไม่มีความเสี่ยง
1 – 7	ความเสี่ยงน้อย
8 – 14	ความเสี่ยงปานกลาง
15 – 21	ความเสี่ยงสูง

ปัจจัยความเสี่ยง:

หัวข้อประเมิน	คะแนนความเสี่ยง			
	0	1	2	3
จำนวนเจ้าของข้อมูล ที่อาจได้รับผลกระทบ	ไม่มีเจ้าของข้อมูลที่ได้รับผลกระทบ เช่น จำนวนข้อมูล ที่รั่วไหล เป็นจำนวนสถิติ หรือข้อมูลที่ได้รับ การแปลงแล้ว	ทราบจำนวนเจ้าของข้อมูลแน่นอน ซึ่งไม่เกิน 10 คน	คาดหมายว่าอาจมีเจ้าของข้อมูลที่ได้รับผลกระทบไม่เกิน 10 คน	มากกว่า 10 คน หรือไม่ สามารถระบุจำนวนเจ้าของข้อมูลได้
ลักษณะของข้อมูล ที่รั่วไหล	ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เช่น ข้อมูลนิรนาม และข้อมูลภาพรวมเชิงสถิติ เป็นต้น และข้อมูลทั่วไปที่สามารถระบุตัวบุคคลได้ แต่เป็นข้อมูลที่ไม่อยู่ภายใต้กำกับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น ข้อมูลของผู้ถึงแก่กรรม ข้อมูลเพื่อกิจกรรมในครอบครัว เป็นต้น	ข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ทันที (โดยไม่รวมถึงข้อมูลอ่อนไหว) ต้องประกอบกับข้อมูลอื่น เช่น รหัสพนักงาน ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น	ข้อมูลส่วนบุคคลที่สามารถระบุตัวเจ้าของข้อมูลได้ทันที เช่น ชื่อของเจ้าของข้อมูล ภาพถ่าย วิดีโอ เป็นต้น	ข้อมูลอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ ความเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลชีวภาพ เป็นต้น
ระยะเวลาการพบการรั่วไหล	ทราบเหตุทันทีที่เกิดการรั่วไหล	ทราบเหตุภายใน 24 ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายใน 24 ชั่วโมง แต่ไม่เกิน 72 ชั่วโมง นับแต่การรั่วไหล	ทราบเหตุภายใน 72 ชั่วโมง นับแต่การรั่วไหล
การเข้าถึงข้อมูลของบุคลากรของบริษัท เมื่อถูกโจรกรรมข้อมูล	บุคลากรสามารถเข้าถึงข้อมูลได้ปกติ	บุคลากรไม่สามารถเข้าถึงข้อมูลบางส่วนเป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมดเป็นการชั่วคราว	บุคลากรไม่สามารถเข้าถึงข้อมูลทั้งหมดเป็นการถาวร

หัวข้อประเมิน	คะแนนความเสี่ยง			
	0	1	2	3
ความเสียหายต่อข้อมูล เมื่อถูกโจรกรรมข้อมูล หรือถูกเข้าโดยไม่ได้รับอนุญาต หรือเกิดจากความผิดพลาดของบุคลากรที่เกี่ยวข้อง	ข้อมูลไม่ได้ถูกแก้ไข / เสียหายประการใด	ข้อมูลถูกแก้ไข แต่ยังไม่ถูกนำไปใช้งาน ซึ่งบริษัท ยังคงมีข้อมูลสำรอง และสามารถใช้อ้างอิงข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งานโดยไม่ทราบว่ามี การแก้ไขข้อมูล ทั้งนี้ บริษัท ยังคงมีข้อมูลสำรอง และสามารถใช้อ้างอิงข้อมูลสำรองได้	ข้อมูลถูกแก้ไข และอาจถูกนำไปใช้งานโดยไม่ทราบว่ามี การแก้ไขข้อมูล ซึ่งบริษัท ไม่มีข้อมูลสำรอง
ขอบเขตในการรั่วไหลของข้อมูล	ข้อมูลไม่ได้ถูกเปิดเผยหรือถูกเข้าถึงโดยมิชอบโดยบุคคลที่ไม่ได้รับอนุญาต	ข้อมูลที่รั่วไหลอาจถูกเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาตภายในบริษัท แต่ยังไม่พบหลักฐานว่าบุคคลที่ไม่ได้รับอนุญาตดังกล่าว มีการประมวลผลโดยมิชอบ เช่น เอกสารหายภายในอาคารบริษัท หรืออุปกรณ์อิเล็กทรอนิกส์ ถูกเลิกใช้งานโดยไม่ลบทำลายข้อมูล	ข้อมูลถูกเปิดเผยหรือเข้าถึงโดยบุคคลภายนอก โดยทราบบุคคลภายนอกดังกล่าว เช่น การส่งอีเมลผิดให้ผู้อื่น พร้อมเอกสารแนบซึ่งเป็นข้อมูลส่วนบุคคล แต่ผู้รับข้อมูลไม่สามารถเปิด หรืออ่านข้อมูลได้ ต้องใช้มาตรการทางเทคนิค จึงจะเข้าถึงข้อมูลได้	ข้อมูลถูกเปิดเผยหรือเข้าถึงโดยบุคคลภายนอกที่ไม่เกี่ยวข้องโดยไม่ทราบจำนวน เช่น ถูกเปิดเผยสาธารณะ หรือ มีการขายข้อมูลลูกค้า/ผู้ถือหุ้นให้กับบุคคลภายนอก
ผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลจากการรั่วไหล	ไม่มีผลกระทบต่อเจ้าของข้อมูล เนื่องจาก เป็นข้อมูลที่เป็นสาธารณะอยู่ก่อนการรั่วไหล หรือ ฝ่ายงานสามารถป้องกันเหตุที่อาจเกิดขึ้นแล้ว	คาดว่าจะไม่เกิดผลกระทบต่อเจ้าของข้อมูล แต่อาจก่อให้เกิดความรำคาญต่อเจ้าของข้อมูล เช่น ต้องกรอกข้อมูลในระบบใหม่ หรือ ลักษณะของข้อมูลที่รั่วไหล ไม่สามารถกระทบต่อการดำรงชีวิตของเจ้าของข้อมูลได้	อาจก่อให้เกิดผลกระทบโดยอ้อม ต่อสิทธิทรัพย์สิน และร่างกาย เช่น เกิดความกลัว หรือ ความกังวล	อาจก่อให้เกิดผลกระทบโดยตรง ที่ไม่อาจแก้ไขได้โดยง่าย เช่น ได้รับความเสียหายต่อทรัพย์สิน ถูกเลิกจ้าง การถูกปฏิเสธในการรับบริการ ถูกดำเนินคดี เสียสุขภาพหรือเจ็บป่วยรุนแรงหรือระยะยาว หรือเสียชีวิต