DIGITAL HEALTH

SISAKET PHO.

1 สำนักงานปลัดกระทรวงฯ ประกาศยุติการให้บริการ e mail 2 โดเมน

ประเด็นพิจารณา

1 กระทรวงไม่ได้กำหนด /จำกัด ผู้ใช้งาน

- ผู้ที่จำเป็นต้องใช้งานจริง เช่น พัสดุ การเงิน หรือ หน่วยที่ต้องใช้ เมลล์ทางการในการติดต่อ
- ใช้เป็นเมลล์ของหน่วยงาน เพื่อความปลอดภัย และ เพิ่มภาพลักษณ์ความน่าเชื่อถือ
- ใช้เป็นเมลล์ของกลุ่มงาน เพื่อความปลอดภัย และ เพิ่มภาพลักษณ์ความน่าเชื่อถือ
- ผู้สนใจในหน่วยงาน

2 เมื่อได้ **Account** แล้วจะสามารถขอใช้พื้นที่ **ONE DRIVE 1 TB** (อาจขอใช้เพิ่มในหนังสือนำส่ง) พร้อม การใช้งาน **office 365 copilot**

วัตถุประสงค์การนำเสนอ

เพื่อทราบ และขอให้แจ้งผู้เกี่ยวข้องดำเนินการ

DIGITAL HEALTH SISAKET PHO.

2 กรณีศึกษาสำนักงานคุ้มครอง ข้อมูลส่วนบุคคล ลงโทษ หน่วยงานภาครัฐและเอกชน เกี่ยวกับการรั่วไหลของ ข้อมูลส่วนบุคคล

ภาพรวมการลงโทษปี 2568

กรณีที่ 1
หน่วยงานรัฐ และบริษัทพัฒนาระบบ

กรณีที่ 2
โรงพยาบาลเอกชน

กรณีที่ 3
ร้านขายคอมพิวเตอร์

กรณีที่ 4
ร้านขายเครื่องสำอาง

กรณีที่ 5
ร้านขายของเล่นสะสม

สรุปเหตุการณ์ [ฉบับย่อ]

• 5 เคส 8 หน่วยงานถูกลงโทษ PDPA ล่าสุด 2568

DBC Group PDPA THAILAND

หน่วยงาน	ประเภท	ลักษณะความผิด	ค่าปรับ (บาท)
หน่วยงานรัฐแห่งหนึ่งที่ให้บริการออนไลน์	รัฐ	ขาดมาตรการความปลอดภัย, ใช้พาสเวิร์ดอ่อนแอ, ไม่ประเมินความเสี่ยง, ละเลยข้อตกลงประมวลผลข้อมูล	153,120
บริษัทผู้พัฒนาและดูแลระบบของหน่วยงานรัฐ	เอกชน	ขาดมาตรการความปลอดภัย, ใช้พาสเวิร์ดอ่อนแอ, ไม่ประเมินความเสี่ยง, ละเลยข้อตกลงประมวลผลข้อมูล	153,120
โรงพยาบาลเอกชนขนาดใหญ่	เอกชน	ปล่อยเอกสารเวชระเบียนหลุด, ไม่ควบคุมกระบวนการทำลายเอกสาร	1,210,000
บุคคลธรรมดา (ผู้รับจ้างทำลายเอกสารโรงพยาบาล)	เอกชน	นำเอกสารไปเก็บที่บ้าน, ไม่แจ้งเหตุรั่วไหล, ไม่ทำตามข้อตกลงกับโรงพยาบาล	16,940
บริษัทขายคอมพิวเตอร์ขนาดใหญ่	เอกชน	ไม่มีมาตรการความปลอดภัย, ไม่แจ้งเหตุรั่วไหล, ไม่มี DPO	7,000,000
บริษัทขายเครื่องสำอาง	เอกชน	ไม่มีมาตรการความปลอดภัย, ไม่แจ้งเหตุรั่วไหล	2,500,000
บริษัทขายของเล่นสะสม	เอกชน	ไม่มีมาตรการรักษาความมั่นคงปลอดภัย แต่มีการเยียวยาผู้เสียหายซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลโดยเร็ว	500,000
บริษัทประมวลผลข้อมูล (ของเล่นสะสม)	เอกชน	ไม่มีมาตรการรักษาความมั่นคงปลอดภัย และไม่มีการตอบสนองที่รวดเร็ว และไม่มีการเยียวยาต่อผู้เสียหาย	3,000,000

กรณีที่ 2 โรงพยาบาลเอกชน

เหตุการณ์

เวชระเบียน 1,000+ ฉบับ
หลุดเป็นถุงขนมโตเกียว

สาเหตุ

ไม่ควบคุมการทำลายเอกสาร

บทลงโทษ

โรงพยาบาล
(Data Controller)
ปรับ 1.2 ล้านบาท

ผู้รับจ้าง
(Data Processor)
ปรับ 1.6 หมื่นบาท

ข้อเสนอแนะเพื่อพิจารณาดำเนินการ

- การตรวจสอบระบบความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน
- หน่วยงานจัดทำรายการข้อมูลส่วนบุคคล และทบทวนสัญญาที่ดำเนินการกับ Vendor ทุกราย
- จัดทำสัญญาดังต่อไปนี้ กับผู้ประมวลผลข้อมูลทุกราย
  - ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement - DPA)
  - ข้อตกลงการรักษาความลับ (Non-Disclosure Agreement - NDA)

เพื่อให้มั่นใจในการปกป้องข้อมูลส่วนบุคคลและการรักษาความลับตามมาตรฐานสากล

DIGITAL HEALTH SISAKET PHO.