Lesson Learned

PDPA

Lesson Learned “PDPA”

Case Study

เคสนี้มีบุคคลที่เกี่ยวข้อง 2 ราย คือ

1. นายสมาน (ลูกค้าและผู้ร้องเรียน) ผู้แจ้งเรื่องผ่านช่องทางของสาขา
2. นาย A (พนักงานสาขา) : ผู้เข้าถึงข้อมูลบัญชีของนายสมาน ผ่านระบบ Web-CSR

ข้อเท็จจริง

1. นายสมาน (ลูกค้าและผู้ร้องเรียน) แจ้งเรื่องผ่านช่องทางสาขา เนื่องจากได้รับหมายศาลมาที่บ้าน โดยในหมายศาลได้ระบุเลขบัญชี (สาขา ก.) และจำนวนเงินในบัญชีธนาคารกรุงไทย (สาขา ก.) ของตนไว้อย่างชัดเจน แต่ตนเองไม่เคยเปิดเผยข้อมูลบัญชีให้บุคคลอื่นทราบ จึงอยากรู้ว่าข้อมูลดังกล่าวถูกเปิดเผยได้อย่างไร
2. จากการตรวจสอบของธนาคารพบว่า นาย A (พนักงานสาขา) ได้มีการเข้าถึงข้อมูลบัญชีของนายสมานผ่านระบบ Web-CSR จริง แต่เข้าไปดูบัญชีของสาขา ข. แต่ไม่พบว่าในบัญชีดังกล่าวมีเงินคงเหลือ

สาเหตุที่ นาย A (พนักงานสาขา) เข้าไปดูข้อมูลทางบัญชีของนายสมาน เนื่องจากต้องการทราบว่านายสมานมีบัญชีร่วมกันกับนางทองผู้ตาย (ป้าของนาย A) หรือไม่ เพื่อที่จะแจ้งให้ทายาทของนางทองทราบ

Case Study

3. ประเด็นที่มาของเลขบัญชี (สาขา ก.) พบว่าข้อมูลดังกล่าว ทนายฝั่งทายาทนางทอง ได้ข้อมูลจากสำนักงานเขต ซึ่งนางทองได้ทำเรื่องสวัสดิการรัฐเบี้ยยังชีพผู้สูงอายุไว้ โดยให้ฝากเข้าบัญชีของนายสมาน (สาขา ก.) ทุกเดือน ในฐานะผู้ดูแล และทนายได้คำนวณจำนวนเงินคร่าวๆ จากเบี้ยยังชีพผู้สูงอายุที่ได้รับทั้งหมดก่อนเสียชีวิต มิได้เป็นยอดจาก Transaction หรือ Statement ของธนาคารแต่อย่างใด

Lesson Learned “PDPA”

กฎหมาย & ระเบียบที่เกี่ยวข้อง

การกระทำดังกล่าวของนาย A เข้าข่ายเป็นความผิดตาม **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562** มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

นอกจากนั้น ยังไม่เป็นไปตาม **ประกาศธนาคารแห่งประเทศไทย ที่ สกส.2. 4/2563 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)** ตามราชกิจจานุเบกษา ลงวันที่ 3 กันยายน 2563 มีผลบังคับใช้วันที่ 4 กันยายน 2563 ดังนี้

(ข้อ1) การบริหารจัดการ ระบบงานที่เกี่ยวข้องกับการให้บริการแก่ลูกค้าอย่างเป็นธรรม

(ข้อ6) การดูแลข้อมูลของลูกค้า : ข้อมูลของลูกค้าได้รับการดูแลอย่างมั่นคงปลอดภัย มีการคำนึงถึงความเป็นส่วนตัวของลูกค้า และมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

Lesson Learned "PDPA"

ระเบียบที่เกี่ยวข้อง

ผิดวินัย ตามระเบียบปฏิบัติงานที่ วพส.340/2568 หมวด HR เรื่อง วินัยและโทษทางวินัย
(ข้อ 2.3) ต้องตั้งใจ ปฏิบัติหน้าที่การงานให้เป็นไปตามกฎหมาย ระเบียบ และคำสั่งของธนาคาร ให้เกิดผลดีหรือความก้าวหน้าแก่ธนาคาร ด้วยความเอาใจใส่ ระมัดระวังรักษาผลประโยชน์ของธนาคาร

(ข้อ 2.12) ต้องรักษาความลับของธนาคาร ไม่แจ้งแก่บุคคลภายนอกให้ทราบถึงกิจการต่างๆ ทั้งของธนาคารและของลูกค้า เว้นแต่ได้รับอนุมัติจากกรรมการผู้จัดการใหญ่ หรือระบุไว้เป็นอย่างอื่น

มาตรฐานโทษทางวินัย

นาย A ได้รับโทษทางวินัยด้วยการตัดเงินเดือนร้อยละ 5 มีกำหนด 3 เดือน

Lesson Learned “PDPA”

ผลกระทบต่อธนาคาร

โทษทางแพ่ง

- ธนาคารอาจจะต้อง**ใช้ค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล** ไม่ว่าจะจงใจให้เกิดเหตุการณ์นั้นขึ้น หรือไม่ตั้งใจก็ตาม

โทษทางปกครอง

- บทลงโทษ PDPA ในทางปกครอง มีอัตราโทษ**ปรับทางปกครองสูงสุดไม่เกิน 5,000,000 บาท**

โทษทางอาญา

- การกระทำความผิดนั้น อาจทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย **ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ**
- การกระทำความผิดนั้น เกิดจากการที่ธุรกิจแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่นโดยทุจริต **ต้องระวางโทษ จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ**
- ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม PDPA แล้วนำไปเปิดเผยแก่ผู้อื่น **ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ**
- ในกรณีที่ผู้กระทำผิดเป็นนิติบุคคล บุคคลที่กระทำความผิด**ต้องรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นๆ และรับโทษตามความผิดนั้นๆ**

Lesson Learned “PDPA”

Do and Don’t

Do ที่พนักงานต้องถือปฏิบัติอย่างเคร่งครัด	Don’t ที่พนักงานต้องถือปฏิบัติอย่างเคร่งครัด
• พนักงานต้องเข้าใจถึงวัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคล • พนักงานเก็บข้อมูลเท่าที่เพียงพอต่อการใช้งาน • พนักงานต้องนำข้อมูลส่วนบุคคลมาใช้ให้ถูกต้องตามวัตถุประสงค์ • พนักงานต้องปฏิบัติตามกฎหมาย และข้อบังคับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎระเบียบและนโยบายที่เกี่ยวข้องของธนาคารอย่างเคร่งครัด	พนักงานต้องไม่กระทำการเก็บรวบรวม ใช้ เปิดเผยซึ่งข้อมูลส่วนบุคคลของบุคคลใดๆ เว้นแต่เป็นการปฏิบัติตามหน้าที่หรือ ได้รับอนุญาตจากผู้บังคับบัญชาล่วงหน้าก่อนแล้ว