กรณีศึกษา PDPA (Case Studies)

- การลบทำลายข้อมูล
- การทำข้อมูลนิรนาม
- การทำเป็นข้อมูลแฝง

ปัจจุบันคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออก ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 ภายใต้พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งมีผลบังคับใช้วันที่ 11 พฤศจิกายน 2567 เพื่อให้องค์กรต่างๆ และ**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** หรือ **DPO** มีแนวทางการนำประกาศนี้ไปใช้ในทางปฏิบัติ บทความนี้เราจึงยกตัวอย่างเคสกรณีศึกษาการลบทำลายข้อมูล การทำข้อมูลนิรนาม และการทำข้อมูลแฝงของบริษัทให้เข้าใจมากยิ่งขึ้น

ก่อนอื่นมาทำความเข้าใจ **การลบทำลายข้อมูล การทำข้อมูลนิรนาม การทำเป็นข้อมูลแฝง** ว่าคืออะไร ควรใช้เมื่อไร และวิธีการทำอย่างไรคร่าว ๆ ดังนี้

1.การลบทำลายข้อมูล (Data Deletion and Destruction) คือการทำให้ข้อมูลสูญหายไปถาวร ไม่สามารถนำกลับมาได้ไม่ว่ากรณีใด ๆ ซึ่งควรใช้ในกรณีต่อไปนี้

1.
    1. ข้อมูลไม่จำเป็นต้องใช้งานอีกต่อไป (เช่น หมดอายุการใช้งานตามที่กฎหมายกำหนด)
    2. เจ้าของข้อมูลร้องขอให้ลบข้อมูล และบริษัทไม่มีเหตุผลทางกฎหมายหรือสัญญาที่จะเก็บข้อมูลนั้นต่อไป
    3. ข้อมูลไม่ถูกต้องหรือมีข้อผิดพลาดและไม่สามารถแก้ไขได้
    4. ครบกำหนดระยะเวลาจัดเก็บตามกฎหมาย

โดยมีวิธีการลบทำลายข้อมูล ได้แก่

1.
    1. ลบข้อมูลออกจากระบบอย่างถาวร (Secure Deletion) เช่น การลบฐานข้อมูลดิจิทัล
    2. ทำลายข้อมูลทางกายภาพ เช่น การหั่นกระดาษ การใช้เครื่องทำลายข้อมูลอิเล็กทรอนิกส์

2.การทำข้อมูลนิรนาม (Anonymization) คือทำให้ข้อมูลเก็บหรือนำไปใช้ได้แต่ไม่สามารถระบุตัวบุคคลได้อีก และไม่มีความเกี่ยวข้องกับตัวบุคคล ไม่ว่าทางตรงและทางอ้อม ควรใช้ในกรณี

1.
    1. บริษัทต้องการเก็บรักษาข้อมูลเพื่อการวิเคราะห์หรือทำวิจัย แต่ไม่ต้องการเก็บข้อมูลส่วนบุคคลในรูปแบบที่สามารถระบุตัวบุคคลได้อีกต่อไป
    2. บริษัทต้องการลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล เมื่อไม่มีเหตุผลในการระบุตัวบุคคลจากข้อมูล เช่น บริษัทต้องการเปิดเผยข้อมูลต่อบุคคลที่สาม หรือต้องการเก็บข้อมูลไว้ใช้ในระยะยาว

ซึ่งมีวิธีการทำให้เป็นข้อมูลนิรนามคร่าว ๆ คือ

1.
    1. ลบข้อมูลที่สามารถระบุตัวบุคคลออกอย่างถาวร แต่ข้อมูลส่วนอื่นยังใช้ประโยชน์ได้
    2. ทำให้ไม่สามารถเชื่อมโยงกลับไปหาเจ้าของข้อมูลได้

3.การทำข้อมูลแฝง (Pseudonymization) คือการทำให้ข้อมูลส่วนบุคคล กลายเป็นข้อมูลแฝงที่ระบุตัวบุคคลไม่ได้ แต่สามารถแปลงหรือสืบค้นกลับได้ ควรใช้ในกรณีต่อไปนี้

1.
    1. บริษัทยังมีความจำเป็นต้องเชื่อมโยงข้อมูลกับบุคคล เช่น การใช้ข้อมูลในการวิเคราะห์หรือการดำเนินการบางอย่าง แต่ไม่ต้องการใช้ข้อมูลที่ระบุตัวบุคคลโดยตรง
    2. บริษัทต้องการลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล แต่ยังสามารถกู้คืนข้อมูลกลับมาเป็นข้อมูลที่ระบุตัวบุคคลได้ในกรณีที่จำเป็น เช่น การใช้หมายเลขหรือตัวระบุที่สามารถเชื่อมโยงกับบุคคลได้หากมีข้อมูลเพิ่มเติม
    3. บริษัทต้องการลดความเสี่ยงในการรั่วไหลของข้อมูล กรณีเป็นการใช้ในกระบวนการภายในบริษัทโดยบุคคลที่ไม่ได้มีความรับผิดชอบต่อข้อมูลโดยตรง
    4. บริษัทต้องการลดความเสี่ยงในการรั่วไหลของข้อมูล กรณีที่มีการโอนข้อมูลให้บุคคลที่สาม ซึ่งมีข้อตกลงในการเปิดเผยข้อมูล

การทำข้อมูลแฝงจะมีวิธีการคร่าวๆดังนี้

1.

1. ใช้การแทนที่ข้อมูลส่วนบุคคลด้วยตัวระบุเฉพาะหรือรหัส โดยสามารถกู้คืนข้อมูลเดิมได้หากจำเป็น
2. เก็บข้อมูลแยกตามชั้นความลับไว้อย่างปลอดภัย

การเลือกใช้วิธีการ **การลบทำลายข้อมูล การทำข้อมูลนิรนาม การทำเป็นข้อมูลแฝง** นั้น ควรคำนึงถึง

1.บริษัทควรพิจารณาเลือกวิธีการที่เหมาะสมตามวัตถุประสงค์ของการประมวลผลข้อมูล และระดับความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยต้องปฏิบัติตามข้อกำหนดของกฎหมาย PDPA อย่างเคร่งครัด

2.บริษัทต้องจัดทำนโยบายและขั้นตอนปฏิบัติที่ชัดเจน

3.ผู้ดำเนินการแต่ละวิธีต้องมีการบันทึกการดำเนินการทุกครั้ง

4.บริษัทและผู้ดำเนินการต้องตรวจสอบประสิทธิภาพของวิธีที่เลือกใช้เป็นระยะ

สำหรับกรณีศึกษาที่จะใช้ทำความเข้าใจ เรื่อง **การลบทำลายข้อมูล การทำข้อมูลนิรนาม การทำเป็นข้อมูลแฝง** ในบทความนี้ จะขอยกตัวอย่าง...

การรับสมัครพนักงานของบริษัทและมีผู้ไม่ผ่านการคัดเลือก ซึ่งบริษัทมีข้อมูลเกี่ยวกับผู้สมัครเป็นพนักงานบริษัทที่ไม่ผ่านการคัดเลือกแบ่งเป็นข้อมูลผู้สมัครที่ไม่ผ่านและไม่เก็บประวัติไว้ กับข้อมูลผู้สมัครที่ไม่ผ่านแต่เก็บประวัติไว้ ดังนั้นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถนำแนวคิดการลบทำลายข้อมูล การทำข้อมูลนิรนาม การทำเป็นข้อมูลแฝง มาประยุกต์ใช้เพื่อให้คำแนะนำในเชิงปฏิบัติได้ดังนี้

1.ข้อมูลผู้สมัครที่ไม่ผ่านและไม่เก็บประวัติไว้ เมื่อบริษัทไม่ต้องการเก็บข้อมูลของผู้สมัครที่ไม่ผ่านการคัดเลือก การจัดการข้อมูลควรดำเนินการใน 2 วิธีดังนี้

1.1 การลบทำลายข้อมูล (Data Deletion and Destruction) เป็นการลบทำลายข้อมูลที่ไม่จำเป็นต่อการคัดเลือกทำงานอย่างถาวร เช่น

1.
    1. ข้อมูลติดต่อ (อีเมล, เบอร์โทรศัพท์)
    2. สำเนาบัตรประชาชน หรือเอกสารอื่นๆ ที่เกี่ยวข้อง
    3. ประวัติส่วนตัวที่ไม่มีความจำเป็นในการเก็บรักษาอีกต่อไป

โดยแนวทางการดำเนินการดังนี้

1.
    1. กำหนดระยะเวลาลบ เช่น 30 วันหลังจากการแจ้งผลการคัดเลือก
    2. จัดทำบันทึกการลบทำลายข้อมูลเพื่อความโปร่งใสในการดำเนินการ

1.2 การทำข้อมูลนิรนาม (Anonymization) หากบริษัทต้องการเก็บข้อมูลเพื่อการวิเคราะห์หรือการวิจัย บริษัทสามารถทำข้อมูลนิรนามเพื่อใช้ในการวิจัยหรือวิเคราะห์ โดยที่ข้อมูลจะไม่สามารถระบุตัวตนได้อีก เช่น

1.
    1. ข้อมูลเชิงสถิติ เช่น ช่วงอายุ, วุฒิการศึกษา, ประสบการณ์ทำงาน, และเหตุผลที่ผู้สมัครไม่ผ่านการคัดเลือก
    2. ข้อมูลที่ระบุตัวบุคคล เช่น ชื่อ ที่อยู่ หรือข้อมูลติดต่อ ควรถูกลบหรือแปลงให้ไม่สามารถระบุตัวบุคคลได้อีก

2.ข้อมูลผู้สมัครที่ไม่ผ่านแต่เก็บประวัติไว้ เมื่อกรณีที่บริษัทต้องการเก็บข้อมูลของผู้สมัครที่ไม่ได้ผ่านการคัดเลือกไว้เพื่อพิจารณาในอนาคตหรือเพื่อวิเคราะห์เพิ่มเติม (โดยมีฐานทางกฎหมายหรือข้อยกเว้นให้สามารถเก็บรักษาไว้ได้) บริษัทควรดำเนินการให้มี Data Security เพิ่มขึ้น ด้วยวิธีการดังนี้

2.1 การทำข้อมูลแฝง (Pseudonymization) หากบริษัทต้องการเก็บข้อมูลไว้ใช้ในการพิจารณาผู้สมัครในอนาคต หรือให้แผนกอื่น ๆ หรือส่งให้บริษัทในเครือ เพื่อพิจารณาเรียกสัมภาษณ์ในภายหลัง สามารถทำข้อมูลแฝงได้ โดยดำเนินการดังนี้

1.
    1. แทนที่ข้อมูลที่สามารถระบุตัวตนได้ (เช่น ชื่อหรือที่อยู่) ด้วยรหัสหรือหมายเลขเฉพาะที่ไม่สามารถระบุตัวบุคคลได้โดยตรง
    2. ข้อมูลที่อาจเก็บไว้ เช่น ประวัติการสัมภาษณ์ คุณสมบัติพิเศษ และผลการประเมิน จะถูกแยกเก็บในที่ปลอดภัย และสามารถเชื่อมโยงกับข้อมูลส่วนตัวได้เมื่อจำเป็น

2.2 การประยุกต์ใช้วิธีการและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลอื่น ๆ เช่น การเก็บรักษาชุดข้อมูลเท่าที่จำเป็น (Data Mininization) โดยลบข้อมูลบางส่วนออกให้เหลือเท่าที่จำเป็นต้องใช้ การเข้ารหัสข้อมูล (Encryption) ผู้เข้าถึงข้อมูลจำเป็นต้องมีรหัสในการเข้าถึง และการกำหนดผู้ที่สามารถเข้าถึงข้อมูล (Data Authorization) เฉพาะผู้เกี่ยวข้องจึงจะสามารถเข้าถึงข้อมูลเท่านั้น เป็นต้น

เงื่อนไขสำคัญในการจัดการข้อมูลของผู้ไม่ผ่านการสมัครตาม PDPA ของบริษัท

1.
    1. บริษัทต้องแจ้งวัตถุประสงค์และระยะเวลาการเก็บ ต่อผู้สมัครอย่างชัดเจนก่อนเก็บข้อมูลหรือทำการประมวลผลใดๆ
    2. ผู้สมัครควรทราบถึงวัตถุประสงค์ของการเก็บข้อมูลและระยะเวลาที่ข้อมูลจะถูกเก็บรักษา
    3. บริษัทให้สิทธิถอนความยินยอมและลบข้อมูล ผู้สมัครมีสิทธิในการขอให้ลบข้อมูลของตนเมื่อข้อมูลนั้นไม่มีความจำเป็นแล้ว
    4. บริษัทมีมาตรการรักษาความปลอดภัยที่เหมาะสม ข้อมูลควรถูกเก็บและประมวลผลภายใต้มาตรการความปลอดภัยที่เข้มงวด เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
    5. บริษัทมีการจำกัดการเข้าถึงข้อมูล ข้อมูลควรเข้าถึงได้เฉพาะผู้ที่จำเป็นต้องใช้เท่านั้น
    6. บริษัทมีการทบทวนความจำเป็นในการเก็บข้อมูล บริษัทควรทบทวนการเก็บข้อมูลเป็นระยะเพื่อให้แน่ใจว่าข้อมูลที่เก็บไว้นั้นยังจำเป็นต่อวัตถุประสงค์ที่ตั้งไว้

การจัดการข้อมูล ด้วยการลบทำลายข้อมูล การทำข้อมูลนิรนาม การทำเป็นข้อมูลแฝง ตามกรณีศึกษานี้จะเกิดผลดังนี้

1.
    1. รักษาประโยชน์ของบริษัท เพราะข้อมูลสามารถใช้ในการพิจารณาผู้สมัครในอนาคตหรือนำไปใช้ในการวิเคราะห์เพื่อปรับปรุงกระบวนการสรรหาต่อไปได้
    2. บริษัทสามารถใช้ประโยชน์จากข้อมูลได้อย่างเหมาะสม การทำข้อมูลนิรนามและการทำข้อมูลแฝงช่วยให้บริษัทยังสามารถใช้ข้อมูลในการวิเคราะห์หรือการพิจารณาผู้สมัครในอนาคตได้โดยไม่ละเมิดสิทธิส่วนบุคคล

3. บริษัทสามารถปฏิบัติตาม PDPA เพราะเป็นการจัดการข้อมูลส่วนบุคคลตามวิธีที่ถูกต้อง ลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคลของผู้สมัคร

————————————————————————

กรณีศึกษานี้จะเน้นการจัดการข้อมูลของผู้สมัครสินเชื่อที่เป็นเพศทางเลือก (LGBTQ+) โดยผู้ควบคุมข้อมูลจากสถาบันการเงิน จะประมวลผลตามสถานการณ์ที่แตกต่างกัน และจัดการข้อมูลใน 3 รูปแบบหลัก ได้แก่ การลบทำลายข้อมูล (Data Deletion and Destruction), การทำข้อมูลนิรนาม (Anonymization) และการทำข้อมูลแฝง (Pseudonymization) เพื่อให้สอดคล้องกับกฎหมายการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรฐานความปลอดภัยข้อมูล

กรณีที่ 1: ผู้สมัครสินเชื่อที่ผ่านการสมัคร และต้องเก็บข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว (เช่น เพศสภาพ)

แนวทางการจัดการข้อมูล

1. การทำข้อมูลนิรนาม (Anonymization):

- ข้อมูลเกี่ยวกับเพศสามารถทำให้เป็นนิรนาม ซึ่งจะทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ โดยไม่ระบุเพศของผู้สมัครเลย
- การทำให้เป็นข้อมูลนิรนามนี้เหมาะสำหรับกรณีที่ไม่จำเป็นต้องทราบเพศเพื่อประมวลผล เช่น การรายงานเชิงสถิติ หรือการวิเคราะห์เชิงภาพรวม

1. การทำข้อมูลแฝง (Pseudonymization):

ข้อมูลเพศสภาพอาจถูกแปลงเป็น Key Identifier หรือใช้ hash เพื่อให้สถาบันการเงินสามารถใช้ข้อมูลนี้ในอนาคตในการประเมินสินค้าและบริการที่เหมาะสม (segmentation) โดยยังคงรักษาความเป็นส่วนตัวของผู้สมัคร

การทำข้อมูลแฝงยังสามารถใช้ในการทำ cross-sale หรือ upsale ให้กับผู้สมัครตามความต้องการที่ตรงกลุ่มเป้าหมายของบริษัท

กรณีที่ 2: ผู้สมัครสินเชื่อที่ไม่ผ่านการสมัคร และไม่ต้องการเก็บข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว

แนวทางการจัดการข้อมูล

1. การลบทำลายข้อมูล (Data Deletion and Destruction):

ในกรณีที่ผู้สมัครไม่ผ่านการสมัครและไม่ต้องการเก็บข้อมูลเพิ่มเติม ข้อมูลส่วนบุคคลทั้งหมดจะต้องถูกลบออกและทำลายให้ไม่สามารถกู้คืนได้ หลังจาก 30 วัน นับจากวันที่ผลอนุมัติสินเชื่อมีผล

วิธีการลบทำลายอาจเป็นการลบแบบที่ไม่สามารถกู้ข้อมูลกลับคืนได้ และ มีรายงานการลบทำลาย เพื่อให้มั่นใจว่าข้อมูลอ่อนไหวไม่สามารถถูกเปิดเผยได้อีกในอนาคต

1. การทำข้อมูลนิรนาม (Anonymization):

อีกวิธีหนึ่งที่สามารถทำได้คือการทำข้อมูลนิรนาม เพื่อให้ข้อมูลที่เหลือไม่สามารถระบุตัวบุคคลได้ และข้อมูลอ่อนไหวเช่น เพศจะไม่ถูกเปิดเผยหรือใช้งานต่อไป

กรณีที่ 3: ผู้สมัครสินเชื่อที่ไม่ผ่านการสมัคร แต่ต้องการเก็บข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว

แนวทางการจัดการข้อมูล

1. การทำข้อมูลแฝง (Pseudonymization):

แม้ว่าผู้สมัครจะไม่ผ่านการสมัคร แต่หากต้องการเก็บข้อมูลเพศในรูปแบบแฝง เพื่อการประเมินสินค้าและบริการในอนาคต (เช่น segmentation) *โดยมีฐานทางกฎหมายหรือข้อยกเว้นให้สามารถเก็บรักษาไว้ได้* ข้อมูลนี้จะถูกแปลงเป็น Key Identifier หรือ hash ซึ่งช่วยให้สามารถวิเคราะห์เชิงกลยุทธ์ได้โดยไม่เปิดเผยข้อมูลตัวตน