ผู้แต่ง : นางสาวกษมพร มหัตเดชกุล นิสิต หลักสูตร นิติศาสตรมหาบัณฑิต สาขาวิชากฎหมายการเงินและภาษีอากร คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

บทความนี้เป็นส่วนหนึ่งของเอกัตศึกษา เรื่อง “การประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคลของธนาคารพาณิชย์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562”

ด้วยเหตุที่ในภาคธุรกิจการเงินจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก และต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ได้มีแนวปฏิบัติ คู่มือ หรือมาตรฐานที่กำหนดสถานการณ์ของเหตุละเมิดว่าสถานการณ์ใดบ้างที่ต้องมีการแจ้งเหตุละเมิดไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล ซึ่งธนาคารพาณิชย์ใช้อ้างอิงปฏิบัติได้ อย่างไรก็ดี การประเมินความเสี่ยงจำเป็นต้องคำนึงถึงประเภทของข้อมูลส่วนบุคคล และมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล ซึ่งมีผลกระทบอย่างสำคัญต่อระดับความเสี่ยง โดยจะทำให้มาตรการตามแนวปฏิบัติ และคู่มือดังกล่าวอาจไม่ใช่มาตรการที่เหมาะสม

จากการศึกษาพบว่าธนาคารพาณิชย์มีการประมวลผลข้อมูลส่วนบุคคล และแยกเป็นประเภทข้อมูลส่วนบุคคลในเบื้องต้นได้ ดังนี้

Group PII	PII
เอกสารหลักฐาน	1. ข้อมูลในบัตรประกันสังคม
เอกสารหลักฐาน	2. ข้อมูลในใบอนุญาตขับขี่รถยนต์

Group PII	PII
เอกสารหลักฐาน	3. ข้อมูลในใบอนุญาตทำงาน
เอกสารหลักฐาน	4. ข้อมูลในใบสำคัญประจำตัวคนต่างด้าว
เอกสารหลักฐาน	5. สำเนาบัตรประจำตัวข้าราชการ / รัฐวิสาหกิจ
เอกสารหลักฐาน	6. สำเนาทะเบียนบ้าน
เอกสารหลักฐาน	7. ใบสำคัญถิ่นที่อยู่
เอกสารหลักฐาน	8. สำเนาใบเปลี่ยนชื่อ
เอกสารหลักฐาน	9. ข้อมูลเกี่ยวกับยานพาหนะหรือหลักประกัน
เอกสารหลักฐาน	10. ปีที่ผลิต ปีที่จดทะเบียน จังหวัดที่จดทะเบียน หมายเลขเครื่องยนต์
เอกสารหลักฐาน	11. บันทึกเลขไมล์
เอกสารหลักฐาน	12. ราคาประเมินทรัพย์สิน
เอกสารหลักฐาน	13. สำเนาเอกสารสิทธิ์หรือสิทธิครอบครองที่ดิน
เอกสารหลักฐาน	14. โฉนดที่ดิน
เอกสารหลักฐาน	15. ข้อมูลเกี่ยวกับทรัพย์สิน
เอกสารหลักฐาน	16. ราคาประเมินทรัพย์สิน
ข้อมูลอัตลักษณ์	17. ชื่อ-นามสกุล
ข้อมูลอัตลักษณ์	18. ชื่อเดิม – นามสกุลเดิม
ข้อมูลอัตลักษณ์	19. คำนำหน้า
ข้อมูลอัตลักษณ์	20. ลายมือชื่อ
ข้อมูลอัตลักษณ์	21. เลขประจำตัวประชาชน
ข้อมูลอัตลักษณ์	22. เลขที่หนังสือเดินทาง
ข้อมูลอัตลักษณ์	23. ภาพถ่าย
ข้อมูลอัตลักษณ์	24. ภาพและ/หรือเสียงจากกล้องวงจรปิด
ข้อมูลอัตลักษณ์	25. หมายเลขประจำตัวลูกค้า
ข้อมูลอัตลักษณ์	26. ลักษณะรูปพรรณสัณฐานบุคคล
ข้อมูลอัตลักษณ์	27. ภาพถ่ายหรือภาพเคลื่อนไหวผ่านกล้องโทรทัศน์วงจรปิด
ข้อมูลประวัติ	28. เพศ
ข้อมูลประวัติ	29. อายุ
ข้อมูลประวัติ	30. วันเดือนปีเกิด
ข้อมูลประวัติ	31. สถานที่เกิด
ข้อมูลประวัติ	32. คุณลักษณะของเจ้าของข้อมูลส่วนบุคคล ส่วนสูง น้ำหนัก
ข้อมูลประวัติ	33. ข้อมูลการเข้าออกประเทศ

Group PII	PII
ข้อมูลประวัติ	34. วันที่จดทะเบียนสมรส
ข้อมูลประวัติ	35. วันที่จดทะเบียนหย่า
ข้อมูลประวัติ	36. สถานภาพทางการสมรส
ข้อมูลประวัติ	37. รายละเอียดเกี่ยวกับการเกณฑ์ทหาร
ข้อมูลประวัติ	38. ทักษะในการใช้ภาษา
ข้อมูลประวัติ	39. ความสัมพันธ์กับกรรมการ ฝ่ายจัดการ และบุคคลผู้มีอำนาจควบคุมของธนาคาร
ข้อมูลประวัติ	40. ความสัมพันธ์กับนิติบุคคลอื่น (เช่น เป็นกรรมการ ฝ่ายบริหารจัดการ ผู้ถือหุ้น)
ข้อมูลประวัติ	41. สถานะการเป็นบุคคลล้มละลาย
ข้อมูลประวัติ	42. ข้อมูลเกี่ยวกับการถูกดำเนินคดี และการถูกบังคับคดี ข้อมูลจากฐานข้อมูลของกรมบังคับคดี
ข้อมูลประวัติ	43. การตรวจพบข้อสงสัยหรือกิจกรรมที่ผิดปกติ
ข้อมูลประวัติ	44. ข้อมูลเกี่ยวกับเชื้อชาติ
ข้อมูลประวัติ	45. ข้อมูลเกี่ยวกับศาสนา
ข้อมูลประวัติ	46. ข้อมูลประวัติอาชญากรรม
ข้อมูลที่อยู่และที่ติดต่อ	47. ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (Email Address)
ข้อมูลที่อยู่และที่ติดต่อ	48. ชื่อหรือบัญชีเข้าใช้งานสำหรับการติดต่อสื่อสารทางอิเล็กทรอนิกส์หรือสื่อสังคมออนไลน์ต่างๆ
ข้อมูลที่อยู่และที่ติดต่อ	49. หมายเลขโทรศัพท์
ข้อมูลที่อยู่และที่ติดต่อ	50. หมายเลขโทรสาร
ข้อมูลที่อยู่และที่ติดต่อ	51. ที่อยู่ตามเอกสารสำคัญ
ข้อมูลที่อยู่และที่ติดต่อ	52. ที่อยู่อาศัยปัจจุบัน
ข้อมูลที่อยู่และที่ติดต่อ	53. ที่อยู่สำหรับการเรียกเก็บเงิน
ข้อมูลเกี่ยวกับการศึกษา	54. รายละเอียดเกี่ยวกับการศึกษาและคุณสมบัติ
ข้อมูลเกี่ยวกับการศึกษา	55. ข้อมูลบนสำเนาบัตรนักศึกษา
ข้อมูลเกี่ยวกับการศึกษา	56. ข้อมูลระดับการศึกษาสูงสุด
ข้อมูลเกี่ยวกับการศึกษา	57. ผลการศึกษา
ข้อมูลเกี่ยวกับการทำงาน	58. บริษัทที่เจ้าของข้อมูลส่วนบุคคลทำงานหรือได้รับการว่าจ้าง
ข้อมูลเกี่ยวกับการทำงาน	59. วันที่ว่าจ้างให้ทำงาน และการบอกเลิกจ้าง
ข้อมูลเกี่ยวกับการทำงาน	60. อาชีพและสาขาอาชีพ

Group PII	PII
ข้อมูลเกี่ยวกับการทำงาน	61. ตำแหน่งการทำงาน ยศ
ข้อมูลเกี่ยวกับการทำงาน	62. สถานภาพทางการเมือง
ข้อมูลเกี่ยวกับการทำงาน	63. อายุงานปัจจุบัน
ข้อมูลเกี่ยวกับการทำงาน	64. เงินเดือน รายได้
ข้อมูลเกี่ยวกับการทำงาน	65. การประเมินต่างๆ (การประเมินผลการทำงานและความเป็นไปได้)
ข้อมูลเกี่ยวกับการทำงาน	66. รายละเอียดงาน ประเภทธุรกิจ
ข้อมูลเกี่ยวกับการทำงาน	67. ข้อมูลความเป็นเจ้าของกิจการ สัดส่วนการถือหุ้น หรือ ข้อมูลบนเอกสารอื่นใดเพื่อยืนยันการประกอบธุรกิจ สัญญาเช่าสถานประกอบกิจการ
ข้อมูลเกี่ยวกับการทำงาน	68. สมาชิกภาพกับองค์กรวิชาชีพ เช่น สมาชิกสภาทนายความ สมาชิกวิศวกรรมสถานแห่งประเทศไทย สมาชิกแพทยสภา
ข้อมูลเกี่ยวกับการทำงาน	69. สถานที่ทำงานเดิม
ข้อมูลเกี่ยวกับการทำงาน	70. เอกสารประกอบการธุรกิจ
ข้อมูลเกี่ยวกับการทำงาน	71. เอกสารการเสียภาษีนิติบุคคล
ข้อมูลเกี่ยวกับการทำงาน	72. ทะเบียนการค้า ภพ.20
ข้อมูลเกี่ยวกับการทำงาน	73. ข้อมูลสหภาพแรงงาน
ข้อมูลเกี่ยวกับครอบครัว	74. สถานภาพครอบครัว
ข้อมูลเกี่ยวกับครอบครัว	75. จำนวนสมาชิกในครอบครัวและจำนวนบุตร
ข้อมูลเกี่ยวกับครอบครัว	76. จำนวนบุตร
ข้อมูลเกี่ยวกับครอบครัว	77. จำนวนบุคคลที่อยู่ในความดูแล
ข้อมูลพฤติกรรม	78. บันทึกการโต้ตอบและการสื่อสารไม่ว่าจะในรูปแบบหรือวิธีใด ๆ เช่น ระหว่างท่านกับธนาคาร ไม่ว่าจะในรูปแบบหรือวิธีใด ๆ ก็ตาม รวมถึงแต่ไม่จำกัดเพียงโทรศัพท์ อีเมล ข้อความสนทนา และการสื่อสารทางสื่อสังคมออนไลน์ การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล ความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล
ข้อมูลพฤติกรรม	79. ประวัติการซื้อของเจ้าของข้อมูลส่วนบุคคล เช่น การซื้อ / เช่า / คืนสินค้า ผลิตภัณฑ์หรือบริการ เงินค่าเช่า ผลประโยชน์ตอบแทน ทรัพย์สินที่ซื้อ (เช่น ประเภททรัพย์ ประเภทเอกสารสิทธิ ราคาขาย ตำแหน่งที่ตั้ง เนื้อที่ แผนที่ และหรือ ข้อมูลอื่น ๆ เกี่ยวกับทรัพย์สินพร้อมขาย ของธนาคารนั้น)
ข้อมูลพฤติกรรม	80. ข้อมูลตำแหน่งภูมิศาสตร์ (geo-location data)
ข้อมูลพฤติกรรม	81. คุกกี้ (Cookies)

Group PII	PII
ข้อมูลพฤติกรรม	82. เว็บบีคอน (Web beacon) พิกเซลแท็ก (Pixel Tag) หรือ Software Development Kit (SDK)
ข้อมูลพฤติกรรม	83. ข้อมูลเกี่ยวกับการค้นหา สถิติการเข้าดู เมนูที่ใช้งาน ระยะเวลาการใช้งานบนเว็บไซต์ แพลตฟอร์ม แอปพลิเคชัน เวลาที่คลิกครั้งสุดท้าย (Timestamp of Last Click) รายการโปรด
ข้อมูลพฤติกรรม	84. ข้อมูลจราจรคอมพิวเตอร์ (Log File)
ข้อมูลพฤติกรรม	85. ข้อมูลการใช้งานและการตอบสนองต่อการโฆษณาของธนาคาร
ข้อมูลพฤติกรรม	86. รายละเอียด Single Sign-on
ข้อมูลพฤติกรรม	87. ข้อมูลการเข้าสู่ระบบ (Log in)
ข้อมูลพฤติกรรม	88. ข้อมูลเกี่ยวกับความสนใจหรือความชื่นชอบส่วนตัว เช่น ลักษณะการใช้งานหรือบริการต่างๆ (รวมถึงการส่งข้อมูลผ่านทางสื่อสังคมออนไลน์หรือการสำรวจความคิดเห็นออนไลน์ คำตอบของเจ้าของข้อมูลส่วนบุคคลต่อคำถาม แบบสอบถาม คำร้องขอทราบข้อเสนอแนะ และการทำวิจัย) ข้อมูลการวิจัยตลาด และข้อมูลการตลาด การสำรวจความคิดเห็นลูกค้า ข้อมูลและความเห็นที่แสดงออกเมื่อเข้าร่วมวิจัยตลาด วิธีการที่ใช้ผลิตภัณฑ์และ/หรือบริการ รวมไปถึงข้อมูลการจ่ายและรับเงิน ความชื่นชอบส่วนบุคคลที่เกี่ยวข้องกับธุรกรรม
ข้อมูลเกี่ยวกับการเงิน	89. ภาระหนี้สินใดที่ติดมากับยานพาหนะ
ข้อมูลเกี่ยวกับการเงิน	90. ข้อมูลเกี่ยวกับผลิตภัณฑ์และ/หรือบริการต่าง ๆ ที่มีอยู่กับธนาคาร (เช่น ข้อมูลบัญชีเงินฝากธนาคาร ข้อมูลบัญชีเงินฝากซึ่งได้แจ้งไว้ประกอบการใช้ผลิตภัณฑ์และ/หรือบริการต่าง ๆ ข้อมูลบัตรเอทีเอ็ม ข้อมูลสินเชื่อ และหลักประกัน ข้อมูลการลงทุน)
ข้อมูลเกี่ยวกับการเงิน	91. ข้อมูลเกี่ยวกับบัญชีเงินฝาก
ข้อมูลเกี่ยวกับการเงิน	92. ข้อมูลเกี่ยวกับบัญชีการลงทุน
ข้อมูลเกี่ยวกับการเงิน	93. ข้อมูลเกี่ยวกับบัตรเครดิต
ข้อมูลเกี่ยวกับการเงิน	94. ข้อมูลเกี่ยวกับบัตรเดบิต
ข้อมูลเกี่ยวกับการเงิน	95. ข้อมูลเกี่ยวกับประกันภัย (เช่น เอกสารคำขอเอาประกันภัย ประเภทการเอาประกันภัย คำขอเอาประกันภัย รายละเอียดข้อมูลกรมธรรม์ประกันภัย วันที่เริ่มและวันที่สิ้นสุดการคุ้มครอง รายละเอียดทรัพย์สินที่เอาประกันภัย เบี้ยประกันภัย ทุนประกันภัย และรายละเอียดการใช้สิทธิเรียกร้องตามกรมธรรม์ประกันภัย)

Group PII	PII
ข้อมูลเกี่ยวกับการเงิน	96. ข้อมูลเกี่ยวกับสินเชื่อ เช่น วัตถุประสงค์ในการสมัครขอสินเชื่อ การชำระเงินดาวน์ ระยะเวลาการชำระเงินดาวน์ วงเงินกู้ อัตราดอกเบี้ย
ข้อมูลเกี่ยวกับการเงิน	97. จำนวนงวดชำระ
ข้อมูลเกี่ยวกับการเงิน	98. ข้อมูลเครดิต
ข้อมูลเกี่ยวกับการเงิน	99. ข้อมูลด้านการเงินและภาษีอากร
ข้อมูลเกี่ยวกับการเงิน	100. ข้อมูลการจัดอันดับความน่าเชื่อถือ
ข้อมูลเกี่ยวกับการเงิน	101. ข้อมูลการปรับปรุงโครงสร้างหนี้
ข้อมูลเกี่ยวกับการเงิน	102. ข้อมูลสำหรับประเมินความเสี่ยง (เช่น ความเหมาะสมในการลงทุน การทำธุรกรรม ความสามารถในการลงทุน การชำระหนี้ หรือการปฏิบัติตามข้อตกลงในการใช้บริการ)
ข้อมูลเกี่ยวกับการเงิน	103. ความรู้เกี่ยวกับการลงทุนและการทำธุรกรรม
ข้อมูลเกี่ยวกับการเงิน	104. ความสามารถในการได้มาและจัดการสินเชื่อ
ข้อมูลเกี่ยวกับการเงิน	105. ประวัติสินเชื่อ ทั้งที่เป็นสินเชื่อของธนาคาร และ/หรือสินเชื่อที่มีอยู่กับสถาบันการเงินอื่น
ข้อมูลเกี่ยวกับการเงิน	106. แหล่งที่มาของรายได้
ข้อมูลเกี่ยวกับการเงิน	107. รายละเอียดข้อตกลงการซื้อขายทรัพย์ วันที่และสถานที่ซื้อทรัพย์ ข้อมูลที่เจ้าของข้อมูลส่วนบุคคลให้ ซึ่งปรากฏอยู่บนแบบฟอร์ม
ข้อมูลเกี่ยวกับการเงิน	108. ข้อมูลสำหรับการปฏิบัติตามกฎหมายป้องกันและปราบปรามการฟอกเงินและตามกฎหมายป้องกันการหลีกเลี่ยงภาษีของประเทศสหรัฐอเมริกา (Foreign Account Tax Compliance Act : FATCA)
ข้อมูลธุรกรรม	109. รายการเคลื่อนไหวในบัญชี
ข้อมูลธุรกรรม	110. ข้อมูลการทำธุรกรรม
ข้อมูลธุรกรรม	111. ข้อมูลรายจ่าย
ข้อมูลธุรกรรม	112. ข้อมูลเกี่ยวกับการชำระหรือรับชำระเงิน
ข้อมูลธุรกรรม	113. บันทึกคำสั่งการทำรายการ
ข้อมูล IT	114. สาขาธนาคารหรือตู้เอทีเอ็มที่ใช้บริการ
ข้อมูล IT	115. หมายเลขประจำเครื่องคอมพิวเตอร์ หรืออินเทอร์เน็ตโพรโทคอล (IP Address)
ข้อมูล IT	116. ที่อยู่ Media Access Control (MAC)
ข้อมูล IT	117. รหัสอุปกรณ์ (Device ID)
ข้อมูล IT	118. ประเภทของอุปกรณ์

Group PII	PII
ข้อมูล IT	119. หมายเลขประจำตัวเครื่อง (Unique Device Identifier: UDID)
ข้อมูล IT	120. หมายเลข IMEI (International Mobile Equipment Identity) ของโทรศัพท์มือถือหรือหมายเลขเฉพาะประจำอุปกรณ์อื่น (unique device identifier)
ข้อมูล IT	121. ชื่อหรือรหัสสำหรับการใช้บริการ (Username)
ข้อมูล IT	122. รหัสผ่านสำหรับใช้ครั้งเดียว (OTP)
ข้อมูล IT	123. ข้อมูล Telemetry
ข้อมูล IT	124. ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลัก (Metadata)
ข้อมูล IT	125. รายละเอียดการเชื่อมต่อประเภท Plug-in ของเบราว์เซอร์ รวมทั้งเวอร์ชั่น การตั้งค่าเขตเวลาและที่ตั้ง
ข้อมูล IT	126. ข้อมูลไร้โครงสร้าง
ข้อมูล IT	127. การระบุเอกลักษณ์ด้วยคลื่นวิทยุ (RFID)
ข้อมูล IT	128. ข้อมูลในอุปกรณ์ MID (เช่น หมายเลขประจำตัวที่แอปพลิเคชัน LINE สร้างขึ้นซึ่งมิใช่ รหัสประจำตัว LINE)
ข้อมูล IT	129. รหัสสำหรับการส่งคำตอบแบบสอบถามผ่านทางแอปพลิเคชัน LINE
ข้อมูลชีวมิติ	130. ข้อมูลชีวภาพ (เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ (fingerprint) การจดจำเสียง (voice recognition) และการจดจำม่านตา (retina recognition))
ข้อมูลสุขภาพ	131. ข้อมูลความพิการ
ข้อมูลสุขภาพ	132. ข้อมูลสุขภาพ (เช่น ข้อมูลน้ำหนัก ส่วนสูง อัตราการเต้นของหัวใจ)
ข้อมูลสุขภาพ	133. กรุ๊ปเลือด
ข้อมูลสุขภาพ	134. ข้อมูลพันธุกรรม

<u>โดยหลัก</u> กฎหมายแบ่งประเภทข้อมูลส่วนบุคคล ได้แก่

ข้อมูลส่วนบุคคล VS. ข้อมูลส่วนบุคคลอ่อนไหว

แต่เมื่อพิจารณาจากความอ่อนไหวของข้อมูลส่วนบุคคลอาจแบ่งประเภทได้มากกว่านั้น ทั้งนี้ เมื่อนำข้อมูลส่วนบุคคลของธนาคารนั้นมาแบ่งประเภทตาม ENISA ได้ดัง<u>ตารางด้านล่าง</u>

ENISA's Group PII	PII
Simple	1. หมายเลขประจำตัวลูกค้า
Simple	2. ชื่อ-นามสกุล
Simple	3. ชื่อเดิม – นามสกุลเดิม
Simple	4. คำนำหน้า
Simple	5. เพศ
Simple	6. อายุ
Simple	7. วันเดือนปีเกิด
Simple	8. สถานที่เกิด
Simple	9. คุณลักษณะของเจ้าของข้อมูลส่วนบุคคล ส่วนสูง น้ำหนัก
Simple	10. ลายมือชื่อ
Simple	11. เลขประจำตัวประชาชน
Simple	12. เลขที่หนังสือเดินทาง
Simple	13. ข้อมูลการเข้าออกประเทศ
Simple	14. วันที่จดทะเบียนสมรส
Simple	15. วันที่จดทะเบียนหย่า
Simple	16. สถานภาพทางการสมรส
Simple	17. สถานภาพครอบครัว
Simple	18. จำนวนสมาชิกในครอบครัวและจำนวนบุตร
Simple	19. รายละเอียดเกี่ยวกับการเกณฑ์ทหาร
Simple	20. ภาพถ่าย
Simple	21. ข้อมูลในบัตรประกันสังคม
Simple	22. ข้อมูลในใบอนุญาตขับขี่รถยนต์
Simple	23. ข้อมูลในใบอนุญาตทำงาน
Simple	24. ข้อมูลในใบสำคัญประจำตัวคนต่างด้าว
Simple	25. สำเนาบัตรประจำตัวข้าราชการ / รัฐวิสาหกิจ
Simple	26. สำเนาทะเบียนบ้าน
Simple	27. ใบสำคัญถิ่นที่อยู่
Simple	28. สำเนาใบเปลี่ยนชื่อ
Simple	29. ทักษะในการใช้ภาษา
Simple	30. รายละเอียดเกี่ยวกับการศึกษาและคุณสมบัติ
Simple	31. ข้อมูลบนสำเนาบัตรนักศึกษา

Simple	32. ข้อมูลระดับการศึกษาสูงสุด
Simple	33. ผลการศึกษา
Simple	34. บริษัทที่เจ้าของข้อมูลส่วนบุคคลทำงานหรือได้รับการว่าจ้าง
Simple	35. วันที่ว่าจ้างให้ทำงาน และการบอกเลิกจ้าง
Simple	36. อาชีพและสาขาอาชีพ
Simple	37. ตำแหน่งการทำงาน ยศ
Simple	38. สถานภาพทางการเมือง
Simple	39. อายุงานปัจจุบัน
Simple	40. การประเมินต่างๆ (การประเมินผลการทำงานและความเป็นไปได้)
Simple	41. รายละเอียดงาน ประเภทธุรกิจ
Simple	42. ข้อมูลความเป็นเจ้าของกิจการ สัดส่วนการถือหุ้น หรือ ข้อมูลบนเอกสารอื่นใดเพื่อยืนยันการประกอบธุรกิจ สัญญาเช่าสถานประกอบกิจการ
Simple	43. สมาชิกภาพกับองค์กรวิชาชีพ เช่น สมาชิกสภาทนายความ สมาชิกวิศวกรรมสถานแห่งประเทศไทย สมาชิกแพทยสภา
Simple	44. สถานที่ทำงานเดิม
Simple	45. เอกสารประกอบการธุรกิจ
Simple	46. เอกสารการเสียภาษีนิติบุคคล
Simple	47. ทะเบียนการค้า ภพ.20
Simple	48. ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (Email Address)
Simple	49. ชื่อหรือบัญชีเข้าใช้งานสำหรับการติดต่อสื่อสารทางอิเล็กทรอนิกส์หรือสื่อสังคมออนไลน์ต่างๆ
Simple	50. หมายเลขโทรศัพท์
Simple	51. หมายเลขโทรสาร
Simple	52. ที่อยู่ตามเอกสารสำคัญ
Simple	53. ที่อยู่อาศัยปัจจุบัน
Simple	54. ความสัมพันธ์กับกรรมการ ฝ่ายจัดการ และบุคคลผู้มีอำนาจควบคุมของธนาคาร
Simple	55. ความสัมพันธ์กับนิติบุคคลอื่น (เช่น เป็นกรรมการ ฝ่ายบริหารจัดการ ผู้ถือหุ้น)
Simple	56. จำนวนบุตร
Simple	57. จำนวนบุคคลที่อยู่ในความดูแล
Simple	58. ภาพและ/หรือเสียงจากกล้องวงจรปิด

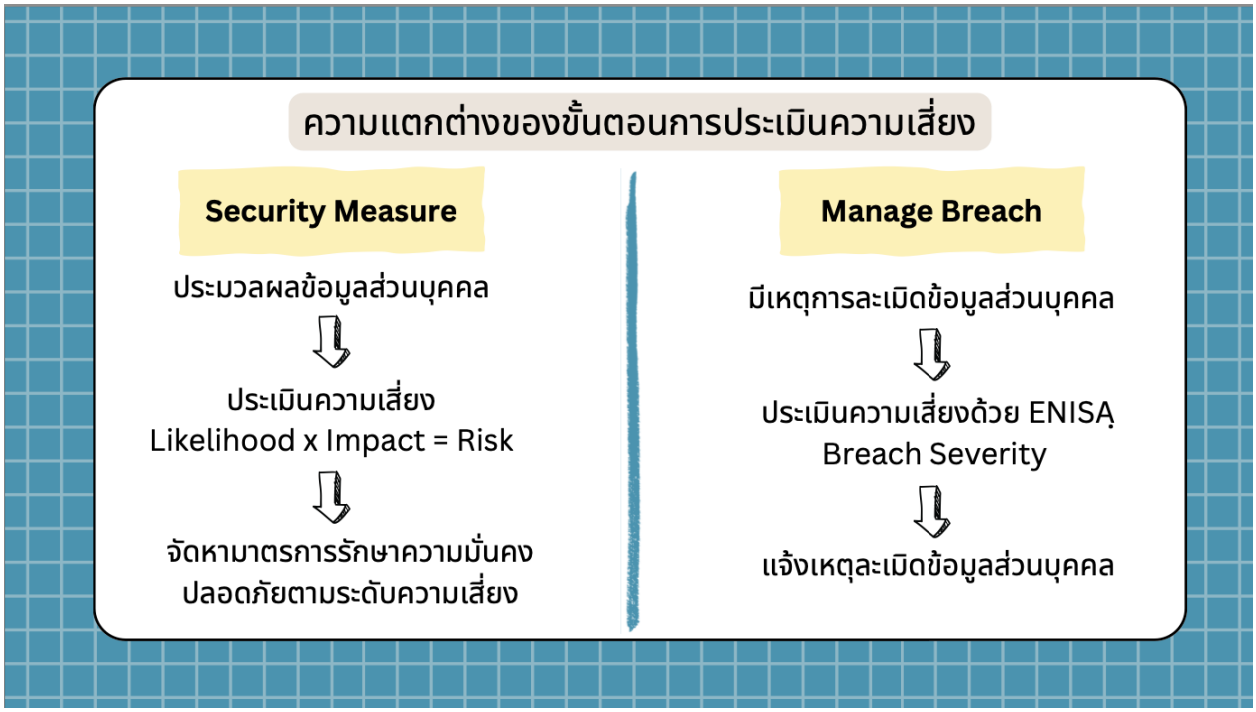
Simple	59. ข้อมูลเกี่ยวกับยานพาหนะหรือหลักประกัน
Simple	60. ปีที่ผลิต ปีที่จดทะเบียน จังหวัดที่จดทะเบียน หมายเลขเครื่องยนต์
Simple	61. บันทึกเลขไมล์
Simple	62. ราคาประเมินทรัพย์สิน
Simple	63. สำเนาเอกสารสิทธิ์หรือสิทธิครอบครองที่ดิน
Simple	64. โฉนดที่ดิน
Simple	65. ข้อมูลเกี่ยวกับทรัพย์สิน
Simple	66. ราคาประเมินทรัพย์สิน
Simple	67. ที่อยู่สำหรับการเรียกเก็บเงิน
Simple	68. สถานะการเป็นบุคคลล้มละลาย
Simple	69. ข้อมูลเกี่ยวกับการถูกดำเนินคดี และการถูกบังคับคดี ข้อมูลจากฐานข้อมูลของกรมบังคับคดี
Simple	70. สาขาธนาคารหรือตู้เอทีเอ็มที่ใช้บริการ
Simple	71. หมายเลขประจำเครื่องคอมพิวเตอร์ หรืออินเทอร์เน็ตโพรโทคอล (IP Address)
Simple	72. ที่อยู่ Media Access Control (MAC)
Simple	73. รหัสอุปกรณ์ (Device ID)
Simple	74. ประเภทของอุปกรณ์
Simple	75. หมายเลขประจำตัวเครื่อง (Unique Device Identifier: UDID)
Simple	76. หมายเลข IMEI (International Mobile Equipment Identity) ของโทรศัพท์มือถือหรือหมายเลขเฉพาะประจำอุปกรณ์อื่น (unique device identifier)
Simple	77. ชื่อหรือรหัสสำหรับการใช้บริการ (Username)
Simple	78. รหัสผ่านสำหรับใช้ครั้งเดียว (OTP)
Simple	79. ข้อมูล Telemetry
Simple	80. ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลัก (Metadata)
Simple	81. รายละเอียดการเชื่อมต่อประเภท Plug-in ของเบราว์เซอร์ รวมทั้งเวอร์ชั่น การตั้งค่าเขตเวลาและที่ตั้ง
Simple	82. ข้อมูลไร้โครงสร้าง
Simple	83. การระบุเอกลักษณ์ด้วยคลื่นวิทยุ (RFID)
Simple	84. ข้อมูลในอุปกรณ์ MID (เช่น หมายเลขประจำตัวที่แอปพลิเคชัน LINE สร้างขึ้นซึ่งมิใช่ รหัสประจำตัว LINE)

Simple	85. รหัสสำหรับการส่งคำตอบแบบสอบถามผ่านทางแอปพลิเคชัน LINE
Simple	86. ลักษณะรูปพรรณสัณฐานบุคคล
Simple	87. การตรวจพบข้อสงสัยหรือกิจกรรมที่ผิดปกติ
Simple	88. ภาพถ่ายหรือภาพเคลื่อนไหวผ่านกล้องโทรทัศน์วงจรปิด
Behavioral	89. บันทึกการโต้ตอบและการสื่อสารไม่ว่าจะในรูปแบบหรือวิธีใด ๆ เช่น ระหว่างท่านกับธนาคาร ไม่ว่าจะในรูปแบบหรือวิธีใด ๆ ก็ตาม รวมถึงแต่ไม่จำกัดเพียงโทรศัพท์ อีเมล ข้อความสนทนา และการสื่อสารทางสื่อสังคมออนไลน์ การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล ความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล
Behavioral	90. ประวัติการซื้อของเจ้าของข้อมูลส่วนบุคคล เช่น การซื้อ / เช่า / คืนสินค้า ผลิตภัณฑ์หรือบริการ เงินค่าเช่า ผลประโยชน์ตอบแทน ทรัพย์สินที่ซื้อ (เช่น ประเภททรัพย์ ประเภทเอกสารสิทธิ ราคาขาย ตำแหน่งที่ตั้ง เนื้อที่ แผนที่ และหรือ ข้อมูลอื่น ๆ เกี่ยวกับทรัพย์สินพร้อมขาย ของธนาคารนั้น)
Behavioral	91. ข้อมูลตำแหน่งภูมิศาสตร์ (geo-location data)
Behavioral	92. คุกกี้ (Cookies)
Behavioral	93. เว็บบีคอน (Web beacon) พิกเซลแท็ก (Pixel Tag) หรือ Software Development Kit (SDK)
Behavioral	94. ข้อมูลเกี่ยวกับการค้นหา สถิติการเข้าดู เมนูที่ใช้งาน ระยะเวลาการใช้งานบนเว็บไซต์ แพลตฟอร์ม แอปพลิเคชัน เวลาที่คลิกครั้งสุดท้าย (Timestamp of Last Click) รายการโปรด
Behavioral	95. ข้อมูลจราจรคอมพิวเตอร์ (Log File)
Behavioral	96. ข้อมูลการใช้งานและการตอบสนองต่อการโฆษณาของธนาคาร
Behavioral	97. รายละเอียด Single Sign-on
Behavioral	98. ข้อมูลการเข้าสู่ระบบ (Log in)
Behavioral	99. ข้อมูลเกี่ยวกับความสนใจหรือความชื่นชอบส่วนตัว เช่น ลักษณะการใช้งานหรือบริการต่างๆ (รวมถึงการส่งข้อมูลผ่านทางสื่อสังคมออนไลน์หรือการสำรวจความคิดเห็นออนไลน์ คำตอบของเจ้าของข้อมูลส่วนบุคคลต่อคำถาม แบบสอบถาม คำร้องขอทราบข้อเสนอแนะ และการทำวิจัย) ข้อมูลการวิจัยตลาด และข้อมูลการตลาด การสำรวจความคิดเห็นลูกค้า ข้อมูลและความเห็นที่แสดงออกเมื่อเข้าร่วมวิจัยตลาด วิธีการที่ใช้ผลิตภัณฑ์และ/หรือบริการ รวมไปถึงข้อมูลการจ่ายและรับเงิน ความชื่นชอบส่วนบุคคลที่เกี่ยวข้องกับธุรกรรม

Financial	100. เงินเดือน รายได้
Financial	101. ภาระหนี้สินใดที่ติดมากับยานพาหนะ
Financial	102. ข้อมูลเกี่ยวกับผลิตภัณฑ์และ/หรือบริการต่าง ๆ ที่มีอยู่กับธนาคาร (เช่น ข้อมูลบัญชีเงินฝากธนาคาร ข้อมูลบัญชีเงินฝากซึ่งได้แจ้งไว้ประกอบการใช้ผลิตภัณฑ์และ/หรือบริการต่าง ๆ ข้อมูลบัตรเอทีเอ็ม ข้อมูลสินเชื่อ และหลักประกัน ข้อมูลการลงทุน)
Financial	103. ข้อมูลเกี่ยวกับบัญชีเงินฝาก
Financial	104. ข้อมูลเกี่ยวกับบัญชีการลงทุน
Financial	105. ข้อมูลเกี่ยวกับบัตรเครดิต
Financial	106. ข้อมูลเกี่ยวกับบัตรเดบิต
Financial	107. ข้อมูลเกี่ยวกับประกันภัย (เช่น เอกสารคำขอเอาประกันภัย ประเภทการเอาประกันภัย คำขอเอาประกันภัย รายละเอียดข้อมูลกรมธรรม์ประกันภัย วันที่เริ่มและวันที่สิ้นสุดการคุ้มครอง รายละเอียดทรัพย์สินที่เอาประกันภัย เบี้ยประกันภัย ทุนประกันภัย และรายละเอียดการใช้สิทธิเรียกร้องตามกรมธรรม์ประกันภัย)
Financial	108. ข้อมูลเกี่ยวกับสินเชื่อ เช่น วัตถุประสงค์ในการสมัครขอสินเชื่อ การชำระเงินดาวน์ ระยะเวลาการชำระเงินดาวน์ วงเงินกู้ อัตราดอกเบี้ย
Financial	109. รายการเคลื่อนไหวในบัญชี
Financial	110. จำนวนงวดชำระ
Financial	111. ข้อมูลการทำธุรกรรม
Financial	112. ข้อมูลรายจ่าย
Financial	113. ข้อมูลเครดิต
Financial	114. ข้อมูลด้านการเงินและภาษีอากร
Financial	115. ข้อมูลการจัดอันดับความน่าเชื่อถือ
Financial	116. ข้อมูลเกี่ยวกับการชำระหรือรับชำระเงิน
Financial	117. ข้อมูลการปรับปรุงโครงสร้างหนี้
Financial	118. ข้อมูลสำหรับประเมินความเสี่ยง (เช่น ความเหมาะสมในการลงทุน การทำธุรกรรม ความสามารถในการลงทุน การชำระหนี้ หรือการปฏิบัติตามข้อตกลงในการใช้บริการ)
Financial	119. ความรู้เกี่ยวกับการลงทุนและการทำธุรกรรม
Financial	120. ความสามารถในการได้มาและจัดการสินเชื่อ

Financial	121. ประวัติสินเชื่อ ทั้งที่เป็นสินเชื่อของธนาคาร และ/หรือสินเชื่อที่มีอยู่กับสถาบันการเงินอื่น
Financial	122. แหล่งที่มาของรายได้
Financial	123. รายละเอียดข้อตกลงการซื้อขายทรัพย์ วันที่และสถานที่ซื้อทรัพย์ ข้อมูลที่เจ้าของข้อมูลส่วนบุคคลให้ ซึ่งปรากฏอยู่บนแบบฟอร์ม
Financial	124. บันทึกคำสั่งการทำรายการ
Financial	125. ข้อมูลสำหรับการปฏิบัติตามกฎหมายป้องกันและปราบปรามการฟอกเงิน และตามกฎหมายป้องกันการหลีกเลี่ยงภาษีของประเทศสหรัฐอเมริกา (Foreign Account Tax Compliance Act : FATCA)
Sensitive	126. ข้อมูลเกี่ยวกับเชื้อชาติ
Sensitive	127. ข้อมูลเกี่ยวกับศาสนา
Sensitive	128. ข้อมูลความพิการ
Sensitive	129. ข้อมูลชีวภาพ (เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ (fingerprint) การจดจำเสียง (voice recognition) และการจดจำม่านตา (retina recognition))
Sensitive	130. ข้อมูลสุขภาพ (เช่น ข้อมูลน้ำหนัก ส่วนสูง อัตราการเต้นของหัวใจ)
Sensitive	131. กรุ๊ปเลือด
Sensitive	132. ข้อมูลพันธุกรรม
Sensitive	133. ข้อมูลสหภาพแรงงาน
Sensitive	134. ข้อมูลประวัติอาชญากรรม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ กำหนดให้ต้องมีการระบุ (Identification) ประเมิน (Assessment) ลด (Mitigate) ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล ในการประมวลผลข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ซึ่งการจัดให้มีมาตรการดังกล่าวนี้ ต้องพิจารณาปัจจัยความเสี่ยงที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลในการประมวลผลข้อมูลส่วนบุคคลนั้นด้วย ในประเทศไทยเองก็มีการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยโดยต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสมซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยง ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล นอกจากนี้ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องประเมินความเสี่ยงว่าเหตุการละเมิดนั้นจะมีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลมากเพียงใดด้วย ดังนั้น จึงแบ่งออกเป็น 2 กรณี

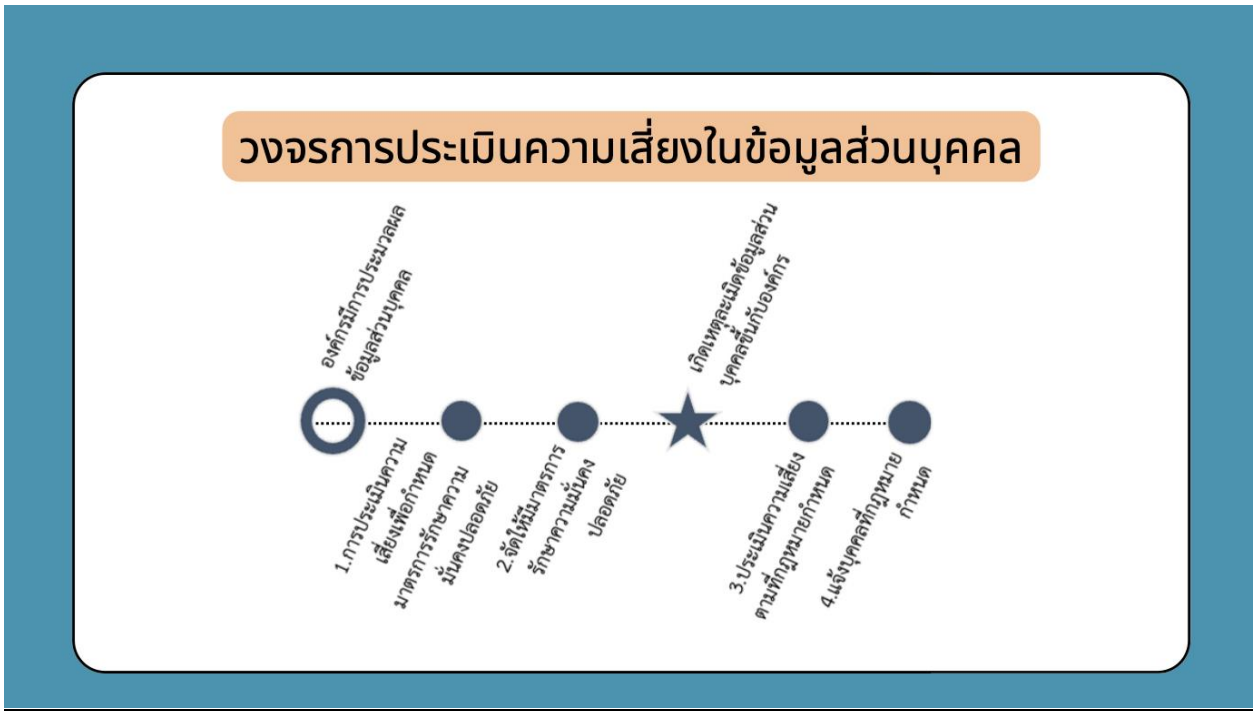


ในแง่มุมของ Security Measure การประเมินความเสี่ยงเป็นหนึ่งในขั้นตอนของการบริหารความเสี่ยง ซึ่งคำนวณระดับความเสี่ยงได้ ด้วยการคำนวณโดยใช้สูตร Likelihood x Impact = Risk เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย เช่น หากประเมินความเสี่ยงได้ในระดับสูง องค์กรอาจควรมีการทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ อย่างน้อยทุก 6 เดือน แต่หากระดับต่ำอาจพิจารณาทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญอย่างน้อยปีละ 1 ครั้ง เป็นต้น

ในแง่มุม Manage Breach เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคลล พ.ร.บ.คุ้มครองข้อมูลฯ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ PDPC เฉพาะกรณีที่การละเมิดมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ต้องเป็นการแจ้งโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ กล่าวคือ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจำต้องพิจารณาก่อนว่าเหตุนั้นมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลหรือไม่ หากไม่มีผลกระทบต่อสิทธิและเสรีภาพ ผู้ควบคุมข้อมูลส่วนบุคคล อาจพิจารณาบันทึกเหตุละเมิดนั้นเพียงกรณีเดียว และไม่จำต้องแจ้งแก่ PDPC หรือเจ้าของข้อมูลส่วนบุคคล แต่หากพิจารณาแล้วเห็นว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลต้องแจ้ง PDPC และเจ้าของข้อมูลส่วนบุคคล ดังสรุปได้ตามตารางด้านล่างนี้

ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล	**ภาระหน้าที่ทางกฎหมาย**
ไม่มีแนวโน้มเสี่ยง	ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งเหตุ แต่อาจพิจารณาบันทึกเหตุละเมิดนั้นได้

ความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล	ภาระหน้าที่ทางกฎหมาย
มีแนวโน้มเสี่ยง	ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุแก่ PDPC ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
มีแนวโน้มเสี่ยงสูง	ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุแก่ PDPC ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
	ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลพร้อมมาตรการเยียวยาโดยไม่ชักช้า



จากการประเมินความเสี่ยงข้างต้น ทั้งการประเมินเพื่อจัดมาตรการรักษาความมั่นคงปลอดภัยและการประเมินเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล สรุปวงจรการประเมินความเสี่ยงได้ตามรูปภาพข้างต้น

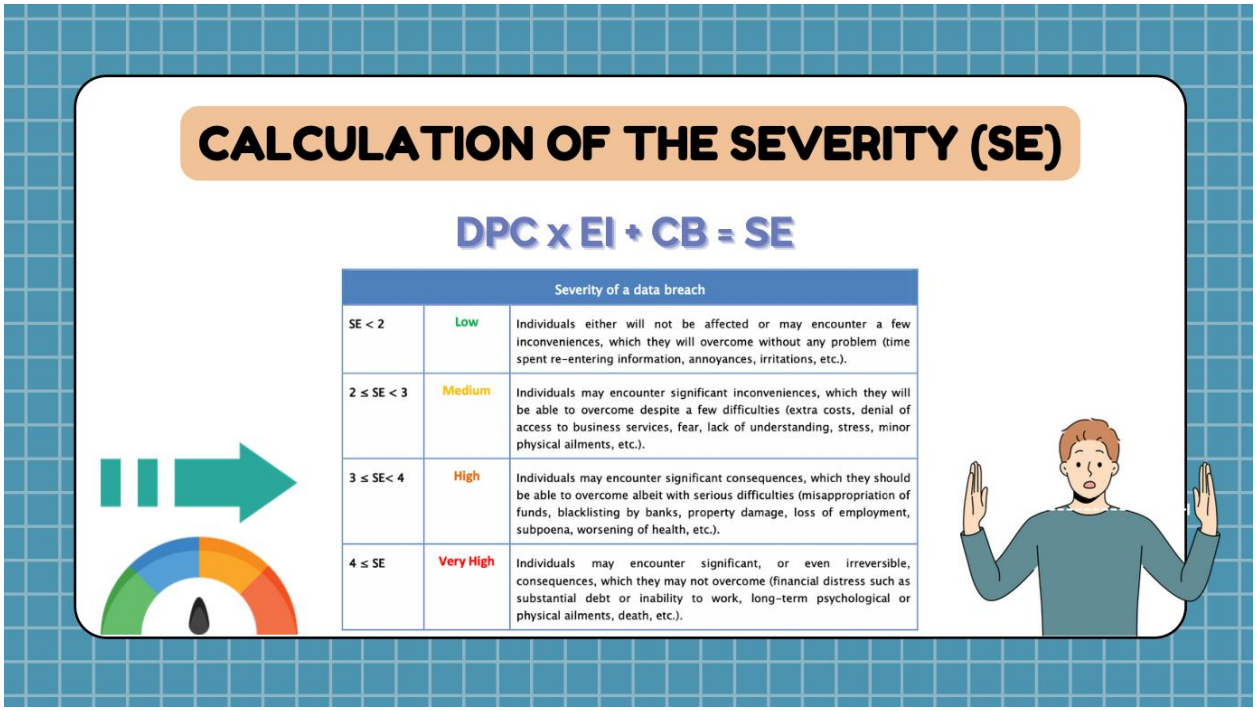
เมื่อคำนวณระดับความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคลแล้ว ให้นำระดับความเสี่ยงไปจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ดังตัวอย่างตามตารางด้านล่างนี้

เลขที่มาตรการ	รายละเอียดมาตรการ	ระดับความเสี่ยง
A.1	องค์กรควรระบุรายละเอียดในนโยบายให้การประมวลผลข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ	เขียว
A.2	ควรมีการทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญอย่างน้อยปีละ 1 ครั้ง เช่นเมื่อองค์กรมีการเปลี่ยนแปลงเทคโนโลยีสารสนเทศที่ใช้งาน เป็นต้น	เขียว
A.3	องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคล นโยบายดังกล่าวควรได้รับการพิจารณาและอนุมัติจากผู้บริหารสูงสุดขององค์กร มีการสื่อสารให้กับทุกคนในองค์กรและหน่วยงานภายนอกที่เกี่ยวข้อง	เหลือง
A.4	นโยบายความมั่นคงปลอดภัยสารสนเทศที่จัดทำควรอ้างอิงถึงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง มาตรการเชิงเทคนิค และมาตรการที่เกี่ยวกับการจัดการองค์กร และหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล หรือหน่วยงานภายนอกอื่นๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	เหลือง

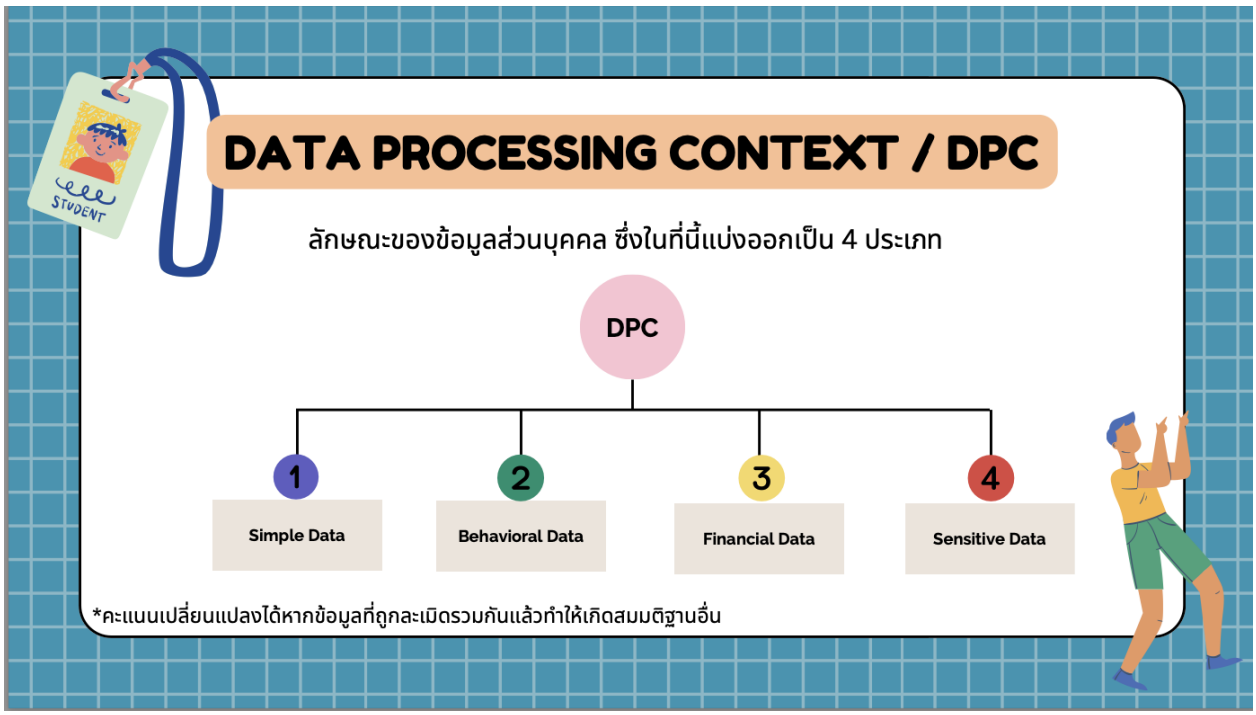
เลขที่มาตรการ	รายละเอียดมาตรการ	ระดับความเสี่ยง
A.5	ควรมีการจัดทำบัญชีรายการเอกสารนโยบาย และขั้นตอนการดำเนินงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	เหลือง
A.6	ควรมีการทบทวนนโยบายเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ อย่างน้อยทุก 6 เดือน	แดง

แนวคิดของ ENISA ได้รับการอ้างอิงในหลากหลายคู่มือ ดังนี้

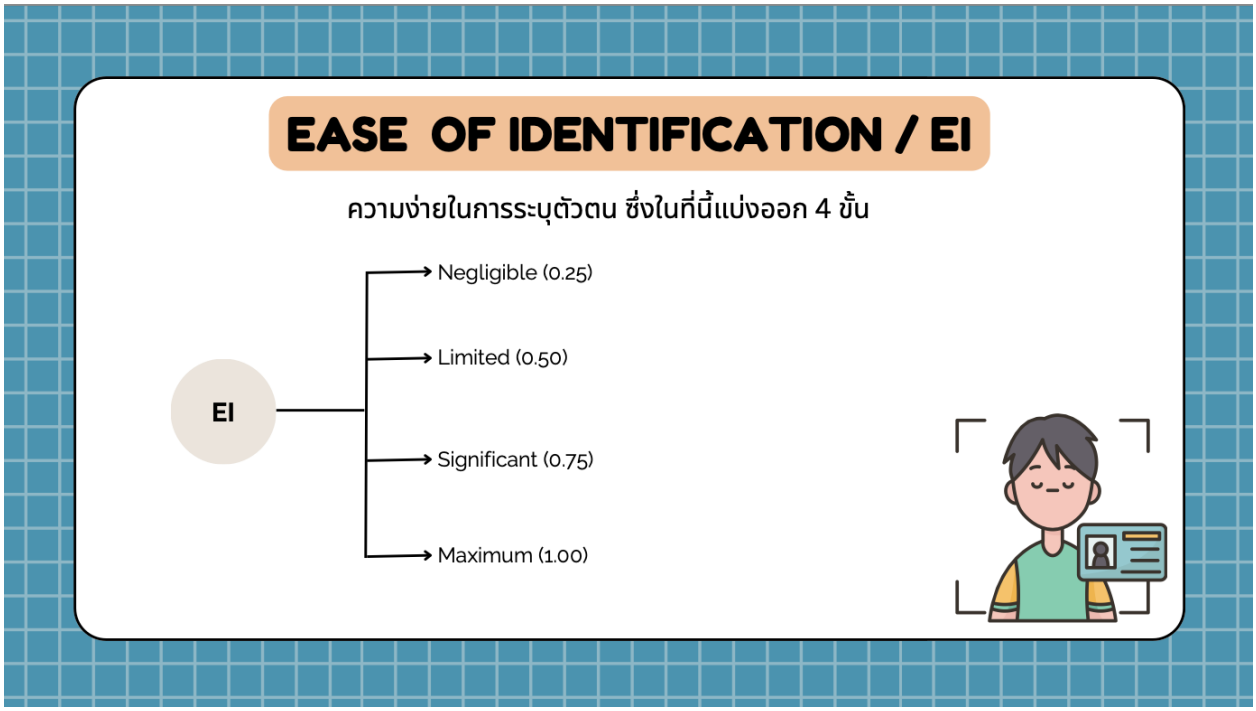
1) คู่มือการแจ้งเหตุละเมิดของ EDPB ที่ชื่อ *Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0* โดยระบุว่า The European Union Agency for Network and Information Security (ENISA) ได้ออกคู่มือระเบียบวิธีการประเมินระดับเหตุการละเมิด ซึ่งผู้ควบคุมข้อมูลส่วนบุคคล สามารถนำไปปรับใช้ในแผนการจัดการเหตุละเมิดของตนได้
2) ICO มีแนะนำให้ค้นคว้ารายละเอียดการประเมินความเสี่ยงตาม ENISA
3) แนวปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ก็มีแนะนำการปรับใช้ ENISA เพื่อมาประเมินระดับความรุนแรงของเหตุการละเมิดข้อมูลส่วนบุคคล



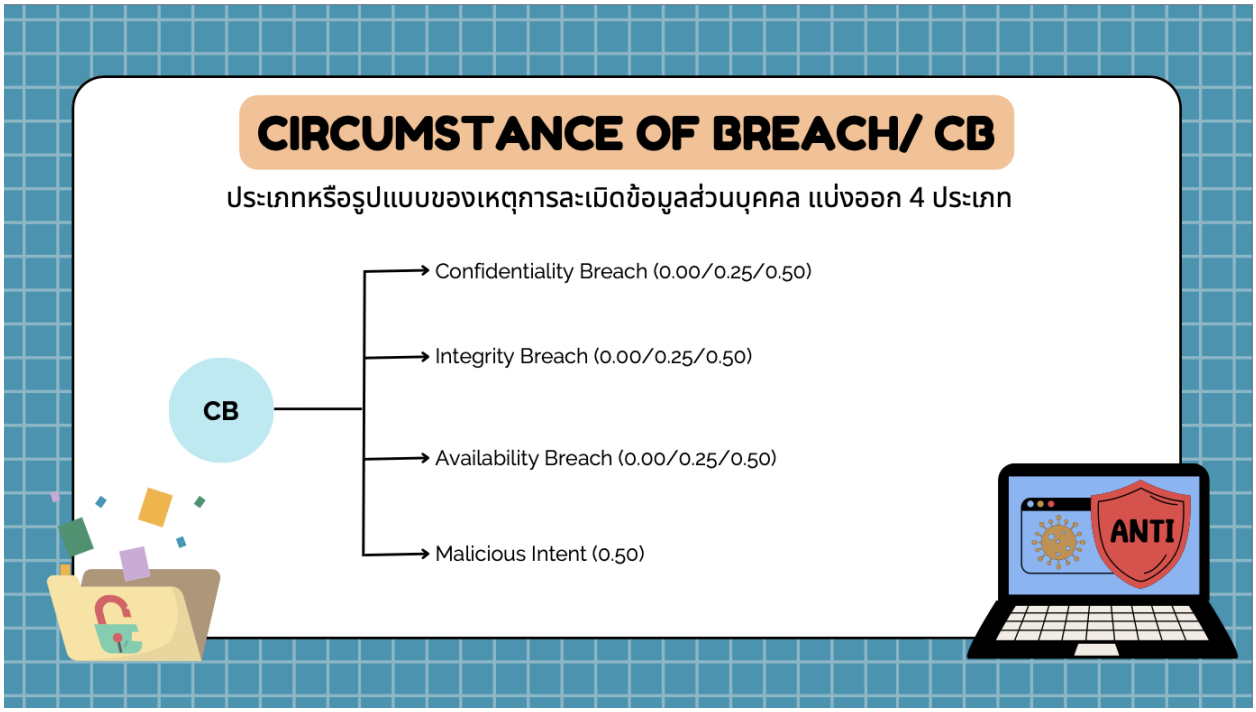
ENISA แบ่งระดับความร้ายแรงของเหตุการละเมิดข้อมูลส่วนบุคคลเป็น 4 ระดับ ซึ่งจะต้องทำการคำนวนจากรายละเอียดของเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น



ENISA แนะนำให้นำข้อมูลส่วนบุคคลที่ถูกละเมิดมาพิจารณาว่ามีระดับความอ่อนไหวเพียงใด โดยแบ่งออกเป็น 4 ประเภทตามรูปข้างต้น เช่น หากเป็นข้อมูลส่วนบุคคลประเภท simple data ก็จะมี score 1 หรือหากมีรายละเอียดอื่นๆ เช่นเป็น simple data ของบุคคลเปราะบางก็ทำให้ score มากขึ้น ซึ่งก็จะส่งผลต่อการคำนวณความร้ายแรงของเหตุการละเมิดข้อมูลส่วนบุคคล ทั้งนี้ รายละเอียดปรากฏตามเอกัตศึกษา



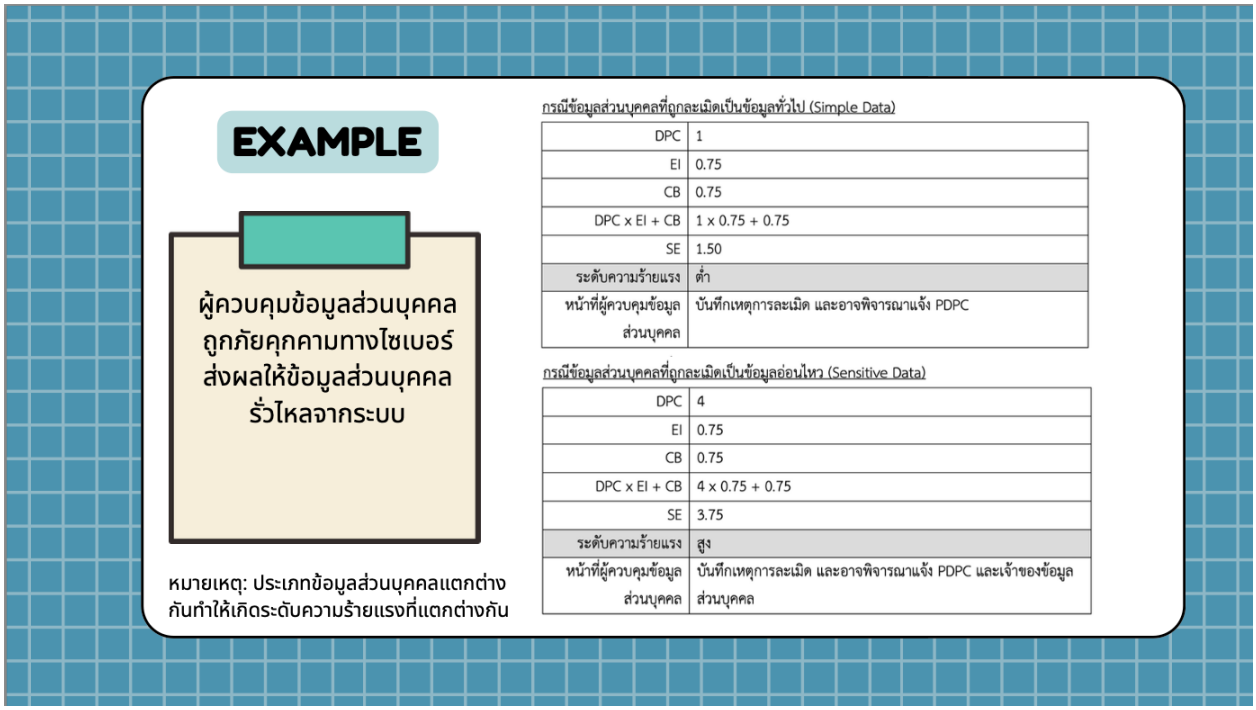
ENISA แนะนำให้พิจารณาว่าข้อมูลส่วนบุคคลที่ถูกละเมิดมีความง่ายในการระบุตัวตนเพียงใด ซึ่ง ENISA ระบุระดับความง่ายในการระบุตัวตน ได้แก่ ข้อมูลชื่อ-นามสกุล ข้อมูลบัตรประชาชน พาสปอร์ต เลขประกันสังคม ข้อมูลเบอร์โทรศัพท์/ข้อมูลสถานที่อยู่อาศัย Email รูปภาพ รหัส/นามแฝง/อักษรย่อ ว่ามีความง่ายในการระบุตัวตนเพียงใด ซึ่งแต่ละข้อมูลแบ่งออกได้ 4 ระดับข้างต้น ทั้งนี้ รายละเอียดปรากฏตามเอกัตศึกษา



ENISA แนะนำให้พิจารณาว่าเหตุการละเมิดข้อมูลส่วนบุคคลเป็นเหตุละเมิดอะไรแบ่งออกเป็น 4 ประเภท โดยแต่ละประเภทจะมีระดับความร้ายแรงของเหตุการณ์ เช่น กรณีที่เกิด Confidentiality Breach โดยข้อมูลส่วน

บุคคลถูกเผยแพร่แก่บุคคลในองค์กรที่ไม่มีสิทธิเข้าถึงข้อมูล ซึ่งจะได้ Score 0.00 หรือ 0.25 จะแตกต่างกับข้อมูลส่วนบุคคลนั้นถูกเผยแพร่ผ่านทางอินเตอร์เน็ต ซึ่งจะได้ Score 0.5 เป็นต้น ทั้งนี้ รายละเอียดปรากฏตามเอกัตศึกษา

ทั้งนี้ ผู้เขียนได้จัดทำรูปแบบการประเมินความร้ายแรงของเหตุการละเมิดข้อมูลส่วนบุคคลทางออนไลน์ โดยนำมาจากแนวคิดของ ENISA ตาม QR Code ข้างต้น



ผู้เขียนได้ประเมินเหตุการละเมิดที่จำลองขึ้นในคู่มือหรือมาตรฐานต่างๆ จากคู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เวอร์ชั่น 1.0 ของ PDPC และแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension) และ Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0 Adopted 28 March 2023 ของ EDPB ทั้งหมด 10 เหตุการณ์ พร้อมเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในภาคการเงินอีก 10 เหตุการณ์ ตัวอย่างเช่น การประเมินเหตุการที่ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบ เหตุการละเมิดที่จำลองในคู่มือไม่ได้ระบุข้อมูลส่วนบุคคลไว้ว่ามีข้อมูลใดบ้างที่ถูกละเมิด และเมื่อนำมาตั้งสมมติฐานว่าหากเป็นข้อมูลทั่วไป และข้อมูลอ่อนไหว จะทำให้เกิดระดับความร้ายแรงที่แตกต่างกันตามรูปข้างต้น

ข้อค้นพบ

แนวปฏิบัติ คู่มือ หรือมาตรฐานที่อธิบายสถานการณ์และระบุมาตรการในการแจ้งเหตุละเมิดต่อ PDPC และเจ้าของข้อมูลส่วนบุคคล มีความเหมาะสมแล้ว เนื่องจากการประเมินใน 10 เหตุการณ์ของผู้เขียน หากมีการประเมินบนสมมติฐานของประเภทข้อมูลส่วนบุคคลที่แตกต่างกันก็อาจส่งผลให้ได้ผลลัพธ์การประเมินสอดคล้อง หรือไม่สอดคล้องกับคู่มือหรือแนวปฏิบัตินั้นก็ได้ หรือหากมีการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย เช่นมีการสำรองข้อมูลส่วนบุคคล ก็ส่งผลให้ระดับความร้ายแรงของเหตุการละเมิดข้อมูลส่วนบุคคลนั้นลดลงได้เช่นกัน นอกจากนี้ แนวปฏิบัติ คู่มือ หรือมาตรฐานเป็นเพียงการแนะแนวให้บุคคลทั่วไปสามารถปฏิบัติตามได้โดยง่าย ผู้ประเมินความเสี่ยงของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลควรต้องพิจารณาปัจจัยที่สำคัญอื่นๆ ด้วย เช่น ข้อมูลส่วนบุคคลที่ถูกละเมิด หรือมาตรการรักษาความมั่นคงปลอดภัยที่ใช้ เป็นต้น