ข้อกำหนดการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล[1] หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

บริษัทได้กำหนดข้อกำหนดการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้เป็นข้อกำหนดกลางของบริษัทในการประเมิน และบริหารจัดการความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้เป็นไปในทิศทางเดียวกัน โดยมุ่งเน้นการพิจารณาความเสี่ยงเฉพาะเรื่องการปฏิบัติการในการประมวลผลข้อมูล (Processing Operation) ครอบคลุมทั้งกระบวนการตั้งแต่การเก็บ(Collect) การเก็บรักษา (Storage) การใช้ (Use) การส่งต่อหรือเปิดเผย (Transfer) และการลบหรือทำลาย (Disposal) ที่อาจจะทำให้เกิดการสูญหาย รั่วไหล หรือละเมิดข้อมูลส่วนบุคคล ซึ่งจะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล การประเมินความเสี่ยงที่กำหนดนี้จะถูกนำไปใช้เป็นข้อมูลในการกำหนดมาตรการป้องกันคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอที่จะทำให้สามารถลดความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลลงต่ำที่สุด และมั่นใจว่าการคุ้มครองป้องกันข้อมุลส่วนบุคคลของบริษัทเป็นไปอย่างมีประสิทธิภาพ เพียงพอ และเหมาะสม
(การละเมิดตามข้อกำหนดนี้ หมายถึง การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ)

1. วัตถุประสงค์

1.1 เพื่อให้มั่นใจว่าการประเมิน และบริหารความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทจะเป็นไปในทิศทางเดียวกัน

1.2 เพื่อให้มั่นใจว่าการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทเป็นไปอย่างเหมาะสม และมั่นใจว่าข้อมูลส่วนบุคคลจะได้รับความคุ้มครองตามที่กฎหมายกำหนด

2. ข้อกำหนดการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

บริษัทได้กำหนดหลักเกณฑ์การประเมิน และการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

[1] มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.1 คำนิยามที่เกี่ยวข้องกับการประเมินความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคล

1) ปัจจัยเสี่ยง (Risk Factor) คือ ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้เกิดการละเมิด หรือรั่วไหลของข้อมูลส่วนบุคคล ซึ่งเกิดได้จากทั้งปัจจัยภายในและภายนอกองค์กร

2) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน

3) การประเมินระดับความรุนแรงของความเสี่ยง (Risk Assessment) เป็นการพิจารณาจากการประเมินระดับความรุนแรงทั้งโอกาสและผลกระทบของปัจจัยเสี่ยงซึ่ง ประกอบด้วยโอกาสและความรุนแรงของผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยระดับความรุนแรงของความเสี่ยง = โอกาสของการเกิดความเสี่ยง (Likelihood) X ระดับของผลกระทบ (Impact)

4) โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

5) ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรง (Severity) ที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหากเกิดเหตุการณ์ความเสี่ยง

6) การตอบสนองความเสี่ยง (Risk Response) เป็นการพิจารณากำหนดแผนงานหรือมาตรการที่จะตอบสนองต่อความเสี่ยงที่เกิดขึ้น

7) การบริหารความเสี่ยง (Risk Management) คือ กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่บริษัทยอมรับได้

8) การติดตามผลและการประเมินผล (Monitoring) เป็นการพิจารณาจากการประเมินผลการควบคุมภายในของบริษัท

2.2 ผู้รับผิดชอบการประเมิน และบริหารจัดการความเสี่ยง

1) ให้ผู้แทนฝ่ายบริหารระบบบริหารคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Management Representative : DPMR) เป็นผู้ประเมินและวิเคราะห์ความเสี่ยงร่วมกับผู้ควบคุมข้อมูล เนื่องจากการวิเคราะห์ความเสี่ยงของข้อมูลส่วนบุคคลเป็นการวิเคราะห์เชิงเทคนิคมาก

2) ให้ผู้ควบคุมข้อมูลเป็นผู้รับผิดชอบในการบริหารจัดการความเสี่ยงในแต่ละปัจจัยเสี่ยงของข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบ โดยอาจมอบหมายให้ผู้ประมวลผลร่วมดำเนินการด้วยก็ได้ และต้องรายงานผลการบริหารจัดการความเสี่ยงให้ DPMR ทราบอย่างน้อยปีละ 2 ครั้ง

3) ให้ DPMR เป็นผู้ติดตาม และประเมินการบริหารจัดการความเสี่ยง และรายงานให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ทราบ และรายงานให้ผู้บริหารทราบในการประชุมทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

2.3 หลักเกณฑ์การประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และความรุนแรงของผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (Impact) จากเหตุการณ์ความเสี่ยงที่เกิดขึ้น

บริษัทจึงได้กำหนดเกณฑ์มาตรฐานในการประเมินความเสี่ยง ทั้งโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ออกเป็น 3 ระดับ เพื่อใช้เป็นเกณฑ์กลางในการประเมินความเสี่ยง ดังนี้

1) เกณฑ์มาตรฐานการประเมินระดับผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (Impact)

บริษัทได้กำหนดเกณฑ์มาตรฐานกลางในการกำหนดระดับความรุนแรงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลที่เกิดจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลซึ่งเป็น**การประเมินข้อมูลเชิงคุณภาพ** โดยแบ่งออกเป็น 3 ระดับ ประกอบด้วย

ระดับผลกระทบ (Level of Impact)	**นิยามผลกระทบ** (Description)
ต่ำ	เจ้าของข้อมูลอาจมีความรู้สึกไม่สะดวก หรือรำคาญเพิ่มขึ้นเล็กน้อยในการที่เขาจะได้รับบริการหรือผลลัพธ์โดยปราศจากปัญหา (เช่น ระยะเวลาในการกรอกข้อมูลใหม่ การถูกรบกวน)
ปานกลาง	เจ้าของข้อมูลมีความรู้สึกไม่สะดวกอย่างมีนัยสำคัญ โดยยังสามารถได้รับบริการหรือผลลัพธ์ถึงแม้จะมีความยากลำบากมากขึ้น (เช่น มีค่าใช้จ่ายเพิ่มเติม การปฏิเสธให้ได้รับการเข้าถึงการใช้บริการทางธุรกิจ ความกลัว ขาดความเข้าใจ ความเครียด)
สูง	เจ้าของข้อมูลพบความยากลำบาก หรือเสียหายมากอย่างมีนัยสำคัญ หรือรู้สึกว่าไม่คุ้มค่าในการรับบริการหรือผลลัพธ์เมื่อเทียบกับความยากลำบากอย่างมาก

	ที่ได้รับ (เช่น ไม่เหมาะสมกับเงิน การถูกขึ้นบัญชีดำ ทรัพย์สินเสียหาย เลิกจ้าง สุขภาพเสียหาย ไม่สามารถทำงานได้ สูญเสียความสามารถทางกายภาพในระยะยาว)

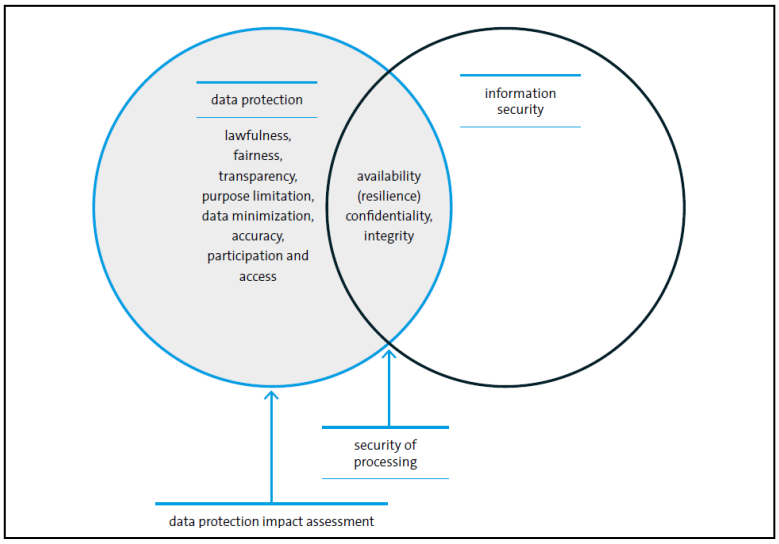
2) เกณฑ์มาตรฐานการประเมินโอกาสที่จะเกิด (Likelihood)

บริษัทได้กำหนดเกณฑ์มาตรฐานกลางในการประเมินโอกาสที่จะเกิดการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลออกเป็น 3 ระดับ ประกอบด้วย

ระดับโอกาสที่จะเกิด (Level of Likelihood)	**นิยามโอกาสที่จะเกิด** (Description)
ต่ำ	โอกาสของภัยคุกคามนี้ต่ำมาก จนถึงไม่น่าจะเกิดขึ้นได้ (มากกว่า 2 ปีต่อครั้ง)
ปานกลาง	มีโอกาสอย่างสมเหตุสมผลที่จะเกิดภัยคุกคามได้ (1 เดือน – 2 ปี ต่อครั้ง)
สูง	โอกาสของภัยคุกคามนี้มีโอกาสบ่อยมาก พบได้ตลอดเวลา หรือสม่ำเสมอ (ต่ำกว่า 1 เดือนต่อครั้ง)

2.4 การประเมินความเสี่ยง (Risk Assessment)

บริษัทได้กำหนดการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล โดยมุ่งเน้นที่ผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เพื่อนำไปใช้ในการออกแบบการป้องกันคุ้มครองข้อมูลส่วนบุคคล จึงได้แบ่งการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลออกเป็น 2 กระบวนการ คือ (ก) การประเมินความเสี่ยงความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (Risk assessment of security of personal data processing) และ (ข) การประเมินผลกระทบการคุ้มครองป้องกันข้อมูล (Data Protection Impact Assessment : DPIA) ที่จะทำในกรณีที่มีผลกระทบรุนแรงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลและการลดความเสี่ยงนั้น



2.4.1 การประเมินความเสี่ยงความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (Risk assessment of security of personal data processing)

บริษัทได้กำหนดขั้นตอนการประเมินความเสี่ยงความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล และการบริหารความเสี่ยง ประกอบด้วย 7 ขั้นตอน ดังนี้

1) การกำหนดเกณฑ์มาตรฐานในการประเมินความเสี่ยง

การกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับผลกระทบของความเสี่ยง (Impact) ซึ่งบริษัทได้กำหนดไว้ตาม 2.3

2) การอธิบายรายละเอียดของการปฏิบัติการประมวลผล (Processing Operation)

ขั้นตอนนี้เป็นการอธิบาย และแยกกระบวนการในการปฏิบัติการประมวลผลข้อมูลของแต่ละข้อมูล เพื่อจะได้นำกระบวนงานทั้งหมดมาพิจารณาหาความเสี่ยงที่จะเกิดขึ้นในกระบวนการทั้งหมด เช่น ชนิดของข้อมูลส่วนบุคคล วัตถุประสงค์ในการประมวลผล วิธีการในการใช้ข้อมูล ผู้รับข้อมูล เป็นต้น โดยมีตัวอย่าง ดังนี้

คำอธิบายการปฏิบัติการประมวลผลข้อมูล (Processing Operation Description)	**ระบุชื่อชุดข้อมูลส่วนบุคคล**
ข้อมูลส่วนบุคคลที่ดำเนินการ (Personal Data Processed)	ระบุข้อมูลส่วนบุคคลที่นำมาใช้ดำเนินการ เช่น ข้อมูลในการติดต่อ (ชื่อ สกุล ที่อยู่ เบอร์โทรศัพท์)
วัตถุประสงค์ของการประมวลผล (Processing Purpose)	ระบุ
เจ้าของข้อมูล (Data Subject)	ระบุ เช่น พนักงาน ลูกค้า ผู้รับจ้างเหมาบริการ (ฟรีแลนซ์)
วิธีการประมวลผล (Processing Means)	ระบุ วิธีการประมวลผลด้วยวิธีใด เช่น ผ่านระบบ Payroll
ผู้รับข้อมูล หรือผู้ที่ได้รับการเปิดเผยข้อมูล (Recipients of the Data)	ระบุ ภายในบริษัท คือใคร และภายนอกบริษัท คือใคร
ผู้ประมวลผลข้อมูล (Data Processor Used)	ระบุ

3) **การประเมินระดับผลกระทบ** (Impact)

การประเมินระดับผลกระทบเป็น**การประเมินข้อมูลเชิงคุณภาพ** โดยให้พิจารณาปัจจัยต่างๆ ตามที่มีอยู่ในการปฏิบัติการประมวลผลที่ระบุ เช่น ชนิดของข้อมูล จำนวนของข้อมูล จุดอ่อนไหวของการประมวลผล เป็นต้น มาประเมินผลกระทบว่าหากมีการสูญหาย รั่วไหล หรือละเมิดข้อมูลจะมีผลกระทบความรุนแรงต่อเจ้าของข้อมูลมากน้อยเพียงใด โดยการประเมินผลกระทบความรุนแรงของปัจจัยเสี่ยงแต่ละปัจจัยนี้ จะแบ่งมิติในการประเมินออกเป็น 3 มิติ คือ

(ก) การสูญเสียการเป็นความลับ (Loss of Confidentiality)

(ข) การสูญเสียความสมบูรณ์ถูกต้องของข้อมูล (Loss of Integrity)

(ค) การสูญเสียในการเข้าถึงการใช้ข้อมูลได้ (Loss of Availability)

โดยให้**พิจารณากำหนดระดับความรุนแรงของผลกระทบตามเกณฑ์มาตรฐานการประเมินระดับผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่กำหนดในข้อ** 2.3 ทั้ง 3 มิติ ตามตารางตัวอย่างคำถามการประเมินระดับผลกระทบ ดังนี้

ลำดับ	คำถาม	ระดับการประเมินผลกระทบ
1	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนดหากเกิดการเปิดเผยข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียการเป็นความลับ)	☐ ต่ำ ☐ ปานกลาง ☐ สูง
2	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนดหากเกิดการแก้ไขข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียความสมบูรณ์ถูกต้องของข้อมูล)	☐ ต่ำ ☐ ปานกลาง ☐ สูง
3	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนดหากเกิดการทำลาย หรือลบข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียการเข้าถึงการใช้ข้อมูลได้)	☐ ต่ำ ☐ ปานกลาง ☐ สูง

การพิจารณาว่าปัจจัยเสี่ยงใดมีผลกระทบความรุนแรงในระดับใด ให้นำผลการพิจารณาผลกระทบทั้ง 3 มิติข้างต้นมาพิจารณา โดยให้กำหนดระดับผลกระทบของปัจจัยเสี่ยงนั้น**ตามระดับความรุนแรงสูงสุดจากที่พบในการประเมินทั้ง 3 มิติ** เช่น

การประเมินผลกระทบความรุนแรง			
มิติการประเมิน	**สูญเสียการเป็นความลับ** (Confidentiality)	**สูญเสียความสมบูรณ์ถูกต้องของข้อมูล** (Integrity)	**สูญเสียการเข้าถึงการใช้ข้อมูลได้** (Availability)
ผลการประเมิน	ปานกลาง	ต่ำ	ต่ำ
สรุปผลการประเมินผลกระทบความรุนแรงของปัจจัยเสี่ยงนี้			**ปานกลาง**

4) การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)

ขั้นตอนนี้เป็นขั้นตอนต่อเนื่องมาจากขั้นตอนที่แล้ว ในการประเมินถึงปัจจัยเสี่ยงต่างๆ หรือภัยคุกคามต่างๆ ที่จะเกิดขึ้นทั้งปัจจัยภายในบริษัทและภายนอกบริษัทนั้น นำมาประเมินโอกาสในการที่จะเกิดขึ้น เพื่อให้การประเมินโอกาสที่ภัยคุกคามนั้นจะเกิดขึ้นมีความง่ายและชัดเจนมากขึ้น จึงได้กำหนดมิติที่เกี่ยวข้องกับภัยคุกคามออกเป็น 4 มิติ ประกอบด้วย

(1) Network and technical resources (ทั้ง hardware และ software)

(2) กระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

(3) ความแตกต่างของคนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

(4) ธุรกิจและขนาดในการประมวลผลข้อมูล

โดยมีตัวอย่างคำถามที่ใช้ในการประเมินโอกาสที่ภัยคุกคามนั้นจะเกิดขึ้น

1. **คำถามเกี่ยวกับ** Network and technical resources		
1.1	มีส่วนใดส่วนหนึ่งการประมวลผลที่ต้องดำเนินการผ่านระบบอินเตอร์เน็ทหรือไม่	การประมวลข้อมูลที่มีส่วนเกี่ยวข้องกับระบบอินเตอร์เน็ทจะมีโอกาสที่จะถูกคุกคามจากภายนอกสูงขึ้น โดยเฉพาะอย่างยิ่ง การให้บริการสำหรับผู้ใช้งานผ่านระบบอินเตอร์เน็ท
1.2	มีโอกาสในการยอมให้มีการเข้าถึงการประมวลผลข้อมูลส่วนบุคคลภายในบริษัท	เมื่อมีการยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคลภายในบริษัทจากอินเตอร์เน็ทจะทำให้มีโอกาส

	จากระบบอินเตอร์เน็ทหรือไม่	ที่ภัยคุกคามจะเกิดสูงขึ้น
1.3	ระบบประมวลผลข้อมูลส่วนบุคคลมีการเชื่อมโยงกับระบบสารสนเทศภายนอกหรือระบบอื่นๆ ภายในบริษัทหรือไม่	การเชื่อมโยงกับระบบสารสนเทศภายนอกบริษัทจะทำให้โอกาสที่จะเกิดภัยคุกคามสูงขึ้น เช่นเดียวกับการเชื่อมโยงกับระบบอื่นๆ ภายในบริษัทก็จะทำให้ผู้ไม่มีอำนาจมีโอกาสเข้าถึงข้อมูลสูงขึ้น
1.4	ผู้ไม่มีอำนาจอื่นๆ สามารถเข้าถึงกระประมวลผลข้อมูลได้อย่างง่ายๆ ใช่หรือไม่	การเปิดโอกาสให้ผู้ไม่มีอำนาจเข้าถึงการประมวลผลข้อมูลได้ง่ายๆ ทั้งระบบอิเล็กทรอนิกส์ หรือตู้จัดเก็บเอกสารจะทำให้มีโอกาสเกิดภัยคุกคามสูงขึ้น
1.5	การออกแบบระบบการประมวลผลข้อมูล การดำเนินการ หรือบำรุงรักษาโดยไม่ได้พิจารณาจากแนวปฏิบัติที่ดีเลยใช่หรือไม่	การพิจารณาแนวปฏิบัติที่ดีแล้วนำมาปรับใช้จะทำให้โอกาสเกิดภัยคุกคามลดลง
2. คำถามเกี่ยวกับกระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล		
2.1	การกำหนดบทบาทและหน้าที่ความรับผิดชอบในกระบวนการประมวลผลข้อมูลมีความไม่ชัดเจนใช่หรือไม่	การที่ไม่มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ไม่ชัดเจน รวมถึงอำนาจในการเข้าถึงข้อมูลจะส่งผลให้ผู้ไม่มีอำนาจมีโอกาสในการเข้าถึงข้อมูลสูงขึ้น
2.2	การอนุญาตให้ใช้ระบบ เครือข่าย รวมถึงทรัพยากรมีความคลุมเครือ หรือไม่ชัดเจนใช่หรือไม่	ความคลุมเครือ ไม่ชัดเจน จะทำให้มีโอกาสการใช้อย่างไม่เหมาะสม ซึ่งทำให้มีโอกาสเกิดภัยคุกคามสูงขึ้น การกำหนดนโยบายหรือแนวปฏิบัติจะช่วยลดความเสี่ยงต่ำลง
2.3	พนักงานได้รับอนุญาตในการนำหรือใช้อุปกรณ์ส่วนตัวในการเชื่อมโยงเข้าถึงระบบการประมวลผลข้อมูลหรือไม่	การอนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัวในการเข้าถึงระบบการประมวลผล จะทำให้มีโอกาสการเข้าถึงข้อมูลของผู้ไม่มีอำนาจสูงขึ้น และยังรวมถึงมีการนำไวรัส หรือ Bugs เข้าสู่ระบบง่ายยิ่งขึ้น
2.4	พนักงานได้รับอนุญาตให้ส่งต่อ หรือจัดเก็บข้อมูล ในการประมวลผลข้อมูลจากภายนอกบริษัท	กระบวนการประมวลผลภายนอกบริษัทจะเพิ่มโอกาสของภัยคุกคามมากยิ่งขึ้น เช่น การใช้ WIFI ของภายนอกบริษัท

2.5	กิจกรรมในการประมวลผลที่จะส่งต่อหรือนำออกไปภายนอกมีการกำหนด log files ไว้หรือไม่	การขาดการจัดเก็บข้อมูล และการติดตามที่เหมาะสมจะส่งผลให้โอกาสในการละเมิดข้อมูลสูงขึ้น
3. คำถามเกี่ยวกับความแตกต่างของบุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผล		
3.1	การประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้ระบุจำนวนพนักงานที่ดำเนินการใช่หรือไม่	การประมวลผลข้อมูลที่เปิดกว้างหรือมีจำนวนพนักงานที่เข้าร่วมประมวลผลจำนวนมากจะทำให้มีโอกาสการละเมิดข้อมูลสูงขึ้น
3.2	มีกระบวนการหรือขั้นตอนในการประมวลผลข้อมูลส่วนบุคคลใดที่ให้ที่ปรึกษาหรือบุคคลภายนอกที่ 3 เข้ามาเป็นผู้ประมวลผลข้อมูลหรือไม่	การประมวลผลข้อมูลจากที่ปรึกษา หรือบุคคลที่ 3 ภายนอกบริษัทจะทำให้การควบคุมเป็นไปได้ยากขึ้นก็ทำให้มีโอกาสเกิดภัยคุกคามมากยิ่งขึ้น
3.3	มีข้อกำหนดให้บุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผลข้อมูลที่คลุมเครือไม่ชัดเจนหรือไม่	ถ้าข้อกำหนดใดๆ ในการปฏิบัติไม่ชัดเจนก็จะส่งผลให้ผู้ปฏิบัติอาจดำเนินการใช้ที่ไม่ถูกต้อง เช่น การลบหรือทำลาย ซึ่งจะทำให้โอกาสเกิดภัยคุกคามสูงขึ้น
3.4	บุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผลข้อมูลที่ไม่คุ้นชินกับระบบการป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศหรือไม่	บุคคลที่ไม่ได้ตระหนักถึงจำเป็นของมาตรการทางด้านการป้องกันความมั่นคงปลอดภัย ก็จะทำให้มีโอกาสความเสี่ยงที่จะทำให้ข้อมูลรั่วไหล หรือละเมิดเพิ่มสูงขึ้น
3.5	มีบุคคลที่เกียวข้องกับการปฏิบัติการประมวลผลข้อมูลมีการละเลยการเก็บรักษาข้อมูลอย่างปลอดภัยหรือการทำลายข้อมูลส่วนบุคคลหรือไม่	การละเมิดข้อมูลส่วนบุคคลหลายครั้งเกิดจากการละเลยในการดูแลที่จัดเก็บเอกสารที่ดีเพียงพอ
4. คำถามเกี่ยวกับธุรกิจและขนาดในการประมวลผลข้อมูล		
4.1	ธุรกิจของบริษัทเป็นธุรกิจที่มักจะโดนหรือน่าสนใจที่จะโจมตี หรือโจรกรรมข้อมูลทางอิเล็กทรอนิกส์หรือไม่	เมื่อการโจรกรรมข้อมูลมักจะมีการโจมตี หรือโจรกรรมในธุรกิจบางธุรกิจ หากธุรกิจของบริษัทอยู่ในกลุ่มเหล่านั้นก็จะทำให้มีความโอกาสในการเกิดภัยคุกคามสูงขึ้น

4.2	บริษัทมีการถูกโจมตี หรือโจรกรรมข้อมูลหรือการละเมิดข้อมูลอื่นใดในรอบ 2 ปีหรือไม่	บริษัทที่เคยโดนโจมตี หรือโจรกรมข้อมูล รวมถึงการละเมิดข้อมูลอื่นใด ย่อมมีโอกาสที่จะถูกกระทำซ้ำอีกหากไม่มีมาตรการมารองรับและแก้ไขไว้
4.3	บริษัทได้รับการแจ้งเตือน หรือร้องเรียนเกี่ยวกับระบบความมั่นคงปลอดภัยด้าน IT ภายใน 1 ปีหรือไม่	การได้รับการแจ้งเตือน หรือเรื่องร้องเรียนจะเป็นตัวบ่งชี้ถึงความเข้มแข็งของระบบการป้องกันความมั่นคงปลอดภัย
4.4	การประมวลผลข้อมูลมีการประมวลผลข้อมูลส่วนบุคคลจำนวนมากๆ หรือไม่	จำนวนข้อมูลจะเป็นสิ่งดึงดูดให้นักโจมตีหรือโจรกรรมข้อมูลเข้ามาโจมตี หรือโจรกรรมข้อมูลสูงยิ่งขึ้น
4.5	มีระบบการป้องกันความมั่นคงปลอดภัยที่เป็นแนวปฏิบัติที่ดีให้บริษัทได้พิจารณาความเหมาะสมในการปฏิบัติตามหรือไม่	ธุรกิจเฉพาะบางธุรกิจมีความจำเป็นต้องมีระบบการป้องกันความมั่นคงปลอดภัยโดยเฉพาะหรือไม่

การพิจารณาว่าปัจจัยเสี่ยงใดมีโอกาสเกิดภัยคุกคามในในระดับใด ให้ดำเนินการประเมินโอกาสในการเกิดภัยคุกคามทั้ง 4 มิติ ตามตารางข้างล่างนี้

มิติในการประเมิน	**โอกาสที่จะเกิดภัยคุกคาม**	
	ระดับ	**คะแนน**
Network and technical resources	☐ ต่ำ	1
	☐ ปานกลาง	2
	☐ สูง	3
กระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล	☐ ต่ำ	1
	☐ ปานกลาง	2
	☐ สูง	3
ความแตกต่างของบุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผล	☐ ต่ำ	1
	☐ ปานกลาง	2
	☐ สูง	3
ธุรกิจและขนาดในการประมวลผลข้อมูล	☐ ต่ำ	1
	☐ ปานกลาง	2

	☐ สูง	3

ปัจจัยเสี่ยงใดจะมีโอกาสเกิดภัยคุกคามระดับใดตามเกณฑ์มาตรฐานที่กำหนดจะเป็นไปตามตารางนี้

คะแนนรวมของโอกาสที่จะเกิดภัยคุกคาม	**ระดับโอกาสเกิดภัยคุกคาม**
4-5	ต่ำ
6-8	ปานกลาง
9-12	สูง

5) การประเมินและจัดลำดับความเสี่ยง

เมื่อได้ค่าระดับผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) จากการพิจารณาในข้อ 3) และ 4) แล้ว ให้นำมาประเมินและจัดลำดับความรุนแรงของความเสี่ยงที่มีผลกระทบต่อบริษัท เพื่อพิจารณากำหนดกิจกรรมการบริหารจัดการความเสี่ยงและควบคุมในแต่ละสาเหตุของความเสี่ยงที่สาคัญให้เหมาะสมตามลำดับความรุนแรงของความเสี่ยง โดยบริษัทได้กำหนดระดับความรุนแรงของความเสี่ยง ออกเป็น 3 ระดับ คือ

(1) ระดับความเสี่ยงต่ำ ตามช่องสีเขียว

(2) ระดับความเสี่ยงปานกลาง ตามช่องสีเหลือง

(3) ระดับความเสี่ยงสูง ตามช่องสีแดง

ตามตารางการวิเคราะห์ความเสี่ยงและระดับความรุนแรงของความเสี่ยงนี้

ระดับผลกระทบ (Impact)	**สูง**			
	ปานกลาง			
	ต่ำ			
ระดับโอกาสที่จะเกิดขึ้น (Likelihood)		**ต่ำ**	**ปานกลาง**	**สูง**

บริษัทได้กำหนดขอบเขตของความรุนแรงที่องค์กรยอมรับได้ (Risk Boundary/ Risk Tolerance) อยู่ที่ระดับความเสี่ยงต่ำ

6) การกำหนดการตอบสนองความเสี่ยง และแผนบริหารจัดการความเสี่ยง

ให้ผู้ควบคุมข้อมูลเป็นผู้รับผิดชอบกำหนดแนวทางในการตอบสนองความเสี่ยงในแต่ละปัจจัยเสี่ยงของข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบที่เกิดขึ้น พร้อมกับกำหนดแผนงานในการบริหารจัดการความเสี่ยงให้มีโอกาสต่ำลง หรือมีผลกระทบที่ต่ำลง พร้อมทั้งดำเนินการให้เป็นไปตามแผนงานที่กำหนด

ผู้รับผิดชอบดำเนินการบริหารจัดการความเสี่ยง ต้องพิจารณาและดำเนินการให้ปัจจัยเสี่ยงทั้งหมดจะต้องไม่อยู่ในระดับสูง

ตัวอย่างมาตรการในการดำเนินการเพื่อตอบสนองและลดความเสี่ยงในแต่ละปัจจัยเสี่ยงกำหนดในเอกสารแนบท้าย

7) การติดตามและประเมินผล

ให้ DPMR เป็นผู้ติดตาม และประเมินการบริหารจัดการความเสี่ยงตามแผนบริหารจัดการความเสี่ยงที่กำหนดและรายงานให้ DPO ทราบ และรายงานให้ผู้บริหารทราบในการประชุมทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

2.4.2 **การประเมินผลกระทบการคุ้มครองป้องกันข้อมูล** (Data Protection Impact Assessment : DPIA)

บริษัทได้กำหนดให้งานหรือโครงการใดๆ รวมถึงการทำโครงการใหม่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลจะต้องถูกนำมาประเมินผลกระทบการคุ้มครองข้อมูล (DPIA) และนำไปบริหารจัดการเพื่อลดความเสี่ยงที่จะเกิดขึ้น รวมถึงเมื่อพบว่ามีการละเมิดข้อมูลส่วนบุคคลจะต้องทำการประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลว่าได้รับผลกระทบรุนแรงหรือไม่

1) การประมวลผลข้อมูลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

การประมวลผลข้อมูลส่วนบุคคลใดที่มีโอกาสสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือการประมวลผลข้อมูลส่วนบุคคลที่มีผลกระทบรุนแรง (สูง) ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลจำเป็นต้องดำเนินการประเมินผลกระทบการคุ้มครองข้อมูล (DPIA) โดยการกำหนดเกณฑ์โอกาส และผลกระทบให้เป็นไปตามที่

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด แต่หากไม่มีการกำหนดให้ใช้เกณฑ์มาตรฐานที่บริษัทกำหนดไว้ตามข้อ 2.3 โดยอนุโลม

การประมวลผลข้อมูลส่วนบุคคลที่เป็นการประมวลผลที่มีโอกาสความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และต้องดำเนินการจัดทำ DPIA ประกอบด้วย

(1) การประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ (Systematic and extensive profiling with significant effects) รวมถึงการทำโปรไฟลิ่ง (Profiling) ซึ่งการประมวลผลดังกล่าวส่งผลต่อการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล

(2) การประมวลผลข้อมูลจานวนมากที่เป็นข้อมูลที่อ่อนไหว (Processing of sensitive data on a large scale) เช่น ข้อมูลอาชญกรรม

(3) การตรวจตราและเฝ้าดูพื้นที่สาธารณะขนาดใหญ่ (Public monitoring on a large scale) เช่น ศูนย์การค้า, ห้องประชุม, ถนนและตรอกซอกซอย, ตลาด, สถานีรถไฟ, หรือห้องสมุดสาธารณะ เป็นต้น

นอกจากนี้ ในกรณีที่มีการวางแผนที่จะทำโครงการที่มีการประมวลผลข้อมูลส่วนบุคคลเกี่ยวข้องกับข้อมูลเหล่านี้ควรต้องจัดทำ DPIA ประกอบด้วย

(4) การใช้เทคโนโลยีที่เป็นนวัตกรรมใหม่

(5) การทำโปรไฟลิ่งในประเภทที่เป็นธุรกิจเฉพาะ

(6) การทำโปรไฟล์ของข้อมูลส่วนบุคคลขนาดใหญ่

(7) การติดตามพฤติกรรมหรือสถานที่ของบุคคล

(8) การทำโปรไฟล์ข้อมูลเด็ก

(9) การประมวลผลข้อมูลที่อาจทำให้เกิดภัยต่อร่างกายของบุคคล เป็นต้น

บริษัทได้ทำการประเมินกิจกรรมของบริษัทที่มีโอกาสความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และต้องดำเนินการจัดทำ DPIA ตามหลักเกณฑ์ข้างต้น ไม่พบว่าบริษัทมีกิจกรรมการประมวลผลข้อมูลใดที่จะเข้าหลักเกณฑ์ดังกล่าว จึงไม่มีความจำเป็นต้องทำ DPIA

ถึงแม้ว่าบริษัทไม่จำเป็นต้องทำ DPIA แต่บริษัทได้กำหนดมาตรการในการควบคุมการดำเนินงานทั้งการออกระเบียบปฏิบัติ รวมถึงมีการทำการตรวจสอบภายใน และระเบียบปฏิบัติเมื่อมีเหตุการละเมิดขึ้น เพื่อให้มั่นใจว่าการป้องกันความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลจะไม่ได้อยู่ในระดับที่สูง

2) ขั้นตอนการประเมินผลกระทบการคุ้มครองป้องกันข้อมูล

หากมีกรณีที่บริษัทมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีโอกาสความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และต้องดำเนินการจัดทำ DPIA ให้ดำเนินการ ดังนี้

(1) ให้ผู้ควบคุมข้อมูลดำเนินการจัดทำการอธิบายรายละเอียดของการปฏิบัติการประมวลผล (Processing Operation) เหมือนที่จัดทำตามข้อ 2) ของข้อ 2.4.1

(2) ให้ผู้ควบคุมข้อมูลประเมินความจำเป็น สัดส่วนความเหมาะสม และมาตรการในการตรวจสอบการดำเนินการตามข้อกำหนดต่างๆ (Compliance measures)

(3) ให้ DPMR ร่วมกับผู้ควบคุมข้อมูลทำการระบุและประเมินความเสี่ยงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลทั้ง โอกาสที่จะเกิดขึ้น และผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามหลักเกณฑ์ที่กำหนด

(4) ให้ DPMR ร่วมกับผู้ควบคุมข้อมูลทำการระบุและกำหนดมาตรการในการลดความเสี่ยง

(5) ให้ผู้ควบคุมข้อมูลดำเนินการตามมาตรการลดความเสี่ยงที่กำหนด และรายงานผลให้ DPMR รับทราบทุกไตรมาส

(6) ให้ DPMR เป็นผู้ติดตาม และประเมินการบริหารจัดการตามมาตรการลดความเสี่ยง พร้อมทั้งรายงานให้ DPO ทราบ และรายงานให้ผู้บริหารทราบในการประชุมทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล