# ข้อกำหนดการออกแบบการคุ้มครองป้องกันข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล[1] หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

บริษัทได้กำหนดข้อกำหนดการออกแบบการคุ้มครองป้องกันข้อมูลส่วนบุคคล เพื่อใช้เป็นแนวทางของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในการกำหนดการคุ้มครองป้องกันข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบอย่างเหมาะสมสอดคล้องกับ**การพิจารณาความเสี่ยง** (Risk Based Approach) ตั้งแต่การป้องกันข้อมูล อาทิ การเก็บรักษา ข้อมูล การจัดส่ง และการใช้หรือเปิดเผย เป็นต้น จนถึงการป้องกันอุปกรณ์ต่างๆ การตรวจสอบ และทดสอบระบบ เพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลของบริษัท ทั้งการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบเป็นไปอย่างมีประสิทธิภาพ เพียงพอ และเหมาะสมในการคุ้มครองข้อมูลส่วนบุคคล

## 1. วัตถุประสงค์

1.1 เพื่อให้มั่นใจว่าผู้ควบคุมข้อมูลและผู้ประมวลผลจะกำหนดการคุ้มครองป้องกันข้อมูลส่วนบุคคลได้ตามข้อกำหนดที่กำหนด

1.2 เพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลมีความเพียงพอและเหมาะสม

1.3 เพื่อให้มั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลได้มีการควบคุมการปฏิบัติงานได้อย่างเหมาะสม และเป็นไปตามวัตถุประสงค์ของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

## 2. การออกแบบคุ้มครองป้องกันข้อมูลส่วนบุคคล

บริษัทได้กำหนดแนวทางในการออกแบบคุ้มครองป้องกันข้อมูลส่วนบุคคลขั้นต่ำที่จะให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลนำไปปรับใช้ในการคุ้มครองป้องกันข้อมูลให้ครอบคุมทั้งข้อมูล และอุปกรณ์ตลอดจนการตรวจสอบและทดสอบระบบ เพื่อให้มั่นใจถึงความเพียงพอ และเหมาะสมในการคุ้มครองป้องกันข้อมูลส่วนบุคคล โดยต้องคำนึงถึงความเสี่ยงในแต่ละข้อมูลส่วนบุคคลด้วย ซึ่งผู้ควบคุมข้อมูลและ

[1] มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผู้ประมวลผลสามารถกำหนดมาตรการใดๆ ที่เหมาะสม และเพียงพอในการคุ้มครองป้องกันข้อมูลที่ตนรับผิดชอบ ดังนี้

**2.1 การป้องกันข้อมูล**

การออกแบบการป้องกันข้อมูล กำหนดไว้เป็น 2 รูปแบบตามลักษณะของข้อมูล คือ ข้อมูลที่เป็นเอกสาร (Physical Document) และ ข้อมูลที่เป็นข้อมูลในระบบอิเล็กทรอนิกส์ (Electronics Data) ดังนี้

2.1.1 การป้องกันข้อมูลที่เป็นเอกสาร

การป้องกันข้อมูลที่เป็นข้อมูลเอกสาร ประกอบด้วย

2.1.1.1 การป้องกันเอกสารข้อมูลส่วนบุคคล

1) ผู้ควบคุมข้อมูลหรือผู้ประมวลผลจะต้องเป็นผู้จัดการเอกสารข้อมูลส่วนบุคคลเท่านั้น

2) ผู้ควบคุมข้อมูลหรือผู้ประมวลผลจะต้องมีการป้องกันข้อมูลในการแก้ไข พิมพ์ หรือคัดลอกข้อมูล ยกเว้นข้อมูลที่ต้องพิมพ์ออกมาเพื่อใช้ประกอบการดำเนินการที่เป็นไปตามข้อกำหนดหรือกฎหมาย และต้องทำลายเอกสารข้อมูลที่สำเนาออกไปทันที่หมดความจำเป็นการใช้งาน

2.1.1.2 การป้องกันที่เก็บรักษา (Storage)

1) การเก็บรักษาเอกสารข้อมูลส่วนบุคคล จะต้องเก็บไว้เป็นสัดส่วน และต้องเป็นอุปกรณ์ที่มีการปิดล็อกการเข้าถึงได้

2) ผู้ควบคุมข้อมูลจะเป็นผู้เก็บรักษากุญแจ

2.1.1.3 การส่งต่อข้อมูล

1) การส่งต่อเอกสารข้อมูลส่วนบุคคลต้องส่งโดยตรงให้กับเฉพาะผู้มีอำนาจเข้าถึงข้อมูลนั้นได้เท่านั้น

2) การส่งต่อเอกสารข้อมูลส่วนบุคคลต้องมีการพิมพ์ข้อความลับ หรือ Confidential

2.1.2 การป้องกันข้อมูลที่เป็นข้อมูลในระบบอิเล็กทรอนิกส์

การป้องกันข้อมูลที่เป็นข้อมูลระบบอิเล็กทรอนิกส์ ประกอบด้วย

2.1.2.1 การป้องกันไฟล์ข้อมูล

1) ไฟล์ข้อมูลส่วนบุคคลต้องกำหนดรหัสในการเข้าใช้ไฟล์ข้อมูล (Encryption) โดยรหัสข้อมูลควรต้องประกอบด้วยอักษรตัวใหญ่ตัวเล็กและตัวเลข จำนวนไม่น้อยกว่า 6 ตัวอักษร และหากเป็นข้อมูลอ่อนไหวต้องกำหนดรหัสไม่น้อยกว่า 8 ตัวอักษร

2) ไฟล์ข้อมูลจะต้องมีการป้องกันข้อมูลในการแก้ไข พิมพ์ หรือคัดลอกข้อมูล ยกเว้นข้อมูลที่ต้องพิมพ์ออกมาเพื่อใช้ประกอบการดำเนินการที่เป็นไปตามข้อกำหนดหรือกฎหมาย

3) รหัสข้อมูลต้องเก็บเป็นความลับ โดยการจัดเก็บไว้ในโปรแกรมที่น่าเชื่อถือ

4) ข้อมูลประเภทรหัสผ่านต้องทำการ Hash ข้อมูลรหัสผ่านก่อนการจัดเก็บลงในฐานข้อมูลทุกครั้ง

5) ไฟล์ข้อมูลส่วนบุคคล สามารถใช้งานได้แค่ในส่วนที่บริษัทกำหนดไว้เท่านั้น ห้ามนำไฟล์ข้อมูลส่วนบุคคลออกไปใช้งานนอกเหนือจากงานที่บริษัทกำหนดไว้

2.1.2.2 การป้องกันที่เก็บรักษา และการ Backup ข้อมูล (Storage & Backup)

1) การเก็บรักษาไฟล์ข้อมูลส่วนบุคคล จะต้องเก็บไว้แยกต่างหากจากโฟลเดอร์อื่นๆ หรือฐานข้อมูลอื่นๆ และกำหนดสิทธิในการเข้าถึงข้อมูลนั้น (Access Control) เฉพาะผู้ที่รับผิดชอบเท่านั้น

2) กรณีที่เป็นข้อมูลของลูกค้า หรือการรับจ้างประมวลผล จะต้องเก็บโฟลเดอร์หรือฐานข้อมูลไว้แยกต่างหากของแต่ละลูกค้า หรือการรับจ้างประมวลผล

3) ข้อมูลส่วนบุคคล ข้อมูลของลูกค้า หรือ ข้อมูลที่รับจ้างประมวลผลจะต้องจัดเก็บไว้ในไดร์ฟกลางของบริษัทที่กำหนดไว้เท่านั้น และจัดเก็บใน Server ของบริษัท

4) บริษัทจะทำการ Back up ข้อมูลทุกสัปดาห์

5) บริษัทมีการกำหนด Firewall ในการป้องกันการเข้าถึงระบบ Server ของบริษัทโดยจะมีแต่ผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าใช้งานได้

2.1.2.3 การส่งต่อข้อมูล

1) การส่งต่อไฟล์ข้อมูลส่วนบุคคลต้องส่งผ่านอีเมล์ของบริษัทเท่านั้น

2) การส่งไฟล์ข้อมูลส่วนบุคคลต้องไม่ส่งไปพร้อมกับรหัสการเปิดไฟล์ข้อมูลในอีเมล์ฉบับเดียวกัน โดยอาจพิจารณาการส่งรหัสเข้าไฟล์ข้อมูลไปอีเมลล์อีกฉบับ หรือช่องทางอื่นๆ เช่น ไลน์ โทรศัพท์ เป็นต้น

3) ให้พิจารณาการลดขั้นตอนการส่งไฟล์ข้อมูลผ่านอีเมล์ให้น้อยที่สุด โดยอาจใช้การเข้าถึงไฟล์ที่จัดเก็บไว้ที่ไดร์ฟกลางแทน

2.1.2.4 การแปลงข้อมูลก่อนการส่งต่อนำไปใช้

1) ควรพิจารณาการแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymous Data) หรือข้อมูลนิรนาม (Anonymous Data) ก่อนการจัดส่งข้อมูลให้ผู้ใช้หรือเปิดเผยข้อมูล เพื่อให้ไม่สามารถพิสูจน์ตัวบุคคลของเจ้าของข้อมูลได้

**2.2 การควบคุมอุปกรณ์อิเล็กทรอนิกส์**

2.2.1 ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบบริหารจัดการทรัพย์สินอุปกรณ์อิเล็กทรอนิกส์ของบริษัท (Asset Management) และจะทำการจัดเก็บ และระบุผู้ควบคุมและใช้ รวมถึงการเปลี่ยนแปลงอุปกรณ์อิเล็กทรอนิกส์

2.2.2 จะต้องมีการกำหนดรหัสการใช้งานอุปกรณ์อิเล็กทรอนิกส์

2.2.3 รหัสการใช้งานอุปกรณ์อิเล็กทรอนิกส์ จะต้องประกอบด้วยอักษรตัวใหญ่ตัวเล็กและตัวเลข จำนวนไม่น้อยกว่า 6 ตัว

2.2.4 ผู้ควบคุมข้อมูลและผู้ประมวลผลจะต้องเปลี่ยนรหัสการใช้งานอุปกรณ์อิเล็กทรอนิกส์ทุก 1 เดือน

2.2.5 ผู้ควบควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องตั้ง Standby อุปกรณ์อิเล็กทรอนิกส์ที่ไม่ได้ใช้งานในระยะเวลา 5 นาที

2.2.6 ผู้ควบควบคุมข้อมูลและผู้ประมวลผลข้อมูลห้ามติด หรือเขียนรหัสการใช้งานอุปกรณ์ติดไว้ที่อุปกรณ์อิเล็กทรอนิกส์

2.2.7 ฝ่ายเทคโนโลยีสารสนเทศจะจำกัดอุปกรณ์อิเล็กทรอนิกส์ ที่ไม่ได้รับอนุญาตในการเข้าถึงข้อมูลส่วนบุคคล

2.2.8 ฝ่ายเทคโนโลยีสารสนเทศมีอำนาจในการเข้าถึงอุปกรณ์อิเล็กทรอนิกส์เพื่อจัดการการใช้งานที่ผิดประเภท

**2.3 ความปลอดภัยของอุปกรณ์มือถือ**

2.3.1 ฝ่ายเทคโนโลยีสารสนเทศ จะป้องกันการเข้าถึงโฟลเดอร์และไฟล์ข้อมูลในไดร์ฟกลางของบริษัท ผ่านอุปกรณ์มือถือทั้งหมด ยกเว้นมีเหตุจำเป็นที่จะต้องมีการขออนุมัติจาก ผู้แทนฝ่ายบริหารระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Management Representative : DPMR) เป็นคราวๆ ไป

**2.4 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคล**

การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลจะแบ่งออกตามลักษณะของข้อมูล ดังนี้

2.4.1 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลที่เป็นเอกสาร

1) ผู้ควบคุมข้อมูลจะต้องทำการตรวจสอบที่จัดเก็บเอกสารข้อมูลส่วนบุคคลว่ามีการปิดล็อกตามปกติ หรือ มีการเข้าถึงเอกสารหรือไม่ทุกสัปดาห์

2) หากพบการละเมิดต้องทำการแจ้งให้ DPMR ทราบทันที

2.4.2 การตรวจสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคลที่เป็นไฟล์อิเล็กทรอนิกส์

1) ฝ่ายเทคโนโลยีสารสนเทศจะทำการตรวจสอบ Log ในการเข้าถึงว่ามีผู้ไม่มีอำนาจพยายามเข้าถึงโฟลเดอร์หรือไฟล์ข้อมูลส่วนบุคคลนั้นหรือไม่ ทุก 7 วัน

2) ฝ่ายเทคโนโลยีสารสนเทศจะทำการตรวจสอบ Log ว่ามีผู้ไม่มีอำนาจเข้าถึงโฟลเดอร์หรือไฟล์ข้อมูลส่วนบุคคลหรือไม่ ทุก 7 วัน

3) หากพบการละเมิดต้องทำการแจ้งให้ DPMR ทราบทันที

**2.5 การควบคุมการทำลายหรือลบข้อมูลส่วนบุคคล**

2.5.1 การทำลายหรือลบข้อมูลส่วนบุคคล เป็นส่วนหนึ่งของการป้องกันข้อมูลด้านการเก็บรักษา (Storage) โดยได้กำหนดข้อกำหนด ดังนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคล **จะต้องกำหนดระยะเวลาการเก็บรักษา**ข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบตามความจำเป็นของการใช้งาน หรือตามที่มีกฎหมายอื่นใดกำหนด และเมื่อพ้นระยะเวลาจัดเก็บ หรือ บริษัทไม่มีสิทธิหรือไม่สามารถอ้างฐานในการประมวลผลข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการทำลายข้อมูลส่วนบุคคลนั้นภายใน 30 วันทำการ

**2.6 การทดสอบการคุ้มครองป้องกันข้อมูลส่วนบุคคล**

1) ฝ่ายเทคโนโลยีสารสนเทศจะทำการทดสอบการเข้าถึงโฟลเดอร์ที่จัดเก็บข้อมูลส่วนบุคคลทุก 7 วัน

2) หากพบว่า สามารถเข้าถึงโฟลเดอร์นั้นได้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องแจ้งให้ DPMR ทราบทันที พร้อมทำการแก้ไข

3) ให้ฝ่ายเทคโนโลยีสารสนเทศทำการเสนอแนะระบบที่เหมาะสมเพียงพอในการคุ้มครองป้องกันข้อมูลส่วนบุคคลให้ DPMR ทราบ