

# คู่มือการปฏิบัติงาน

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

บริษัท นีมลีส์ซิ่ง จำกัด



## สารบัญ

	หน้า
คำนำ	ก
คำนิยาม	ข
วัตถุประสงค์	ค
<b>1. แนวทางปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562</b>	<b>1</b>
<b>2. แนวทางปฏิบัติงานการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล</b>	<b>3</b>
2.1. วัตถุประสงค์	3
2.2. ผู้รับผิดชอบ และหน้าที่ความรับผิดชอบ	3
2.3. การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล	3
2.3.1 ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้	3
2.3.2 การขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลหลังที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้	4
2.3.3 ขั้นตอนปฏิบัติงานต่อการเปิดเผยหรือเปลี่ยนแปลงวัตถุประสงค์ในการใช้งาน	5
2.3.4 การขอความยินยอมผ่านคุกกี้ (Cookies)	6
2.4. ขั้นตอนปฏิบัติงานต่อการจัดเก็บความยินยอม	7
2.5. การขอเพิกถอนความยินยอมการใช้ เปิดเผยข้อมูลส่วนบุคคล	7
2.6. การปฏิบัติการณ์ยืนยันตัวตน	8
<b>3. แนวทางปฏิบัติในการเก็บรวบรวมข้อมูลส่วนบุคคล</b>	<b>9</b>
3.1. การควบคุมการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้ำก่อนเข้าทำสัญญา	9
3.2. การเก็บรวบรวมข้อมูลเพิ่มเติม และเก็บรวบรวมข้อมูลจากแหล่งอื่น	9
3.3. การกำหนดและแยกแยะข้อมูลส่วนบุคคล	10
สรุปแนวทางปฏิบัติในการเก็บรวบรวมข้อมูลส่วนบุคคล	12
<b>4. แนวทางปฏิบัติในการใช้และเปิดเผยข้อมูลส่วนบุคคล</b>	<b>14</b>
4.1. การใช้และการเปิดเผยข้อมูลส่วนบุคคล	14
4.2. การควบคุมการใช้งานและการเข้าถึงข้อมูลส่วนบุคคล	15
4.3. การใช้หรือเปิดเผยข้อมูลส่วนบุคคลของแต่ละหน่วยงาน	15
<b>5. แนวทางปฏิบัติในการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล</b>	<b>17</b>
5.1. สิทธิของเจ้าของข้อมูลส่วนบุคคล	17
5.2. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ	17
5.3. ขั้นตอนปฏิบัติงานต่อการแจ้งใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	18
5.4. เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล	20

6. แนวทางปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ	21
6.1. วัตถุประสงค์	21
6.2. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ	21
6.3. ขั้นตอนการปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ	22
7. แนวทางปฏิบัติงานกรณีเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล	23
7.1. วัตถุประสงค์	23
7.2. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ	23
7.3. ขั้นตอนปฏิบัติงานต่อการแจ้งเหตุละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล	23
8. เกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล	25
9. ปัจจัยที่ต้องพิจารณา เพื่อการประเมินความเสี่ยงของข้อมูลส่วนบุคคล	26
10. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล การทำลายข้อมูลตามระยะเวลาที่กำหนด และการปฏิบัติต่อข้อมูลที่มีอยู่ก่อนพระราชบัญญัติบังคับใช้	27
10.1. มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล	27
10.2. การทำลายข้อมูลตามระยะเวลาที่กำหนด	29
11. การร้องเรียน	30
11.1. เจ้าของข้อมูลส่วนบุคคลร้องเรียนต่อบริษัท	30
11.2. เจ้าของข้อมูลร้องเรียนต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล	30
12. สรุปการกำหนดโทษตามกฎหมายนี้	31
12.1. โทษทางแพ่ง	31
12.2. โทษทางอาญา	32
12.3. โทษทางปกครอง	33
13. บทลงโทษ	37
14. การตรวจสอบ ติดตามเพื่อให้พนักงานปฏิบัติตามกฎเกณฑ์ PDPA	37
15. การให้ความรู้แก่พนักงานและการปรับปรุงนโยบายบริษัทให้เป็นไปตาม PDPA	37
16. การทบทวนแนวปฏิบัติ	38
17. การติดต่อสอบถามหรือใช้สิทธิ	38



## คำนำ

เนื่องจากปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลง พัฒนาและก้าวหน้าเป็นอย่างมาก ทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายและเป็น การล่วงละเมิดสิทธิความเป็นส่วนตัวเจ้าของข้อมูลส่วนบุคคลนั้น อีกทั้งก่อให้เกิดความเสียหายต่อบริษัท กระทบต่อความน่าเชื่อถือและภาพลักษณ์ขององค์กร

บริษัท นีมี่สซิ่ง จำกัด ตระหนักและให้ความสำคัญถึงสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูล ส่วนบุคคลของลูกค้า คู่ค้า พันธมิตรทางธุรกิจ ผู้บริหารและบุคลากร ดังนั้นบริษัทจึงได้จัดทำคู่มือในการ ปฏิบัติงานเกี่ยวกับการจัดการข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อเป็นการสร้างกลไก หลักเกณฑ์ มาตรการกำกับ ดูแลและแนวทางปฏิบัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบุคคลดังกล่าวแล้วข้างต้น



## คำนิยาม

**บริษัทฯ** หมายถึง บริษัท นีมลีสซิ่ง จำกัด

**ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

**ข้อมูลส่วนบุคคลอ่อนไหว** หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

**เจ้าของข้อมูลส่วนบุคคล** หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล ที่บริษัทฯ เก็บรวบรวม ใช้ หรือเปิดเผย แต่ไม่ใช่กรณีที่บุคคลที่ครอบครองข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง

**ประเภทของเจ้าของข้อมูลส่วนบุคคล** หมายถึง เจ้าของข้อมูลส่วนบุคคลที่บริษัทฯ เก็บและประมวลผลข้อมูลส่วนบุคคล ได้แก่ ลูกค้า คู่สัญญา ซัพพลายเออร์ ผู้ขาย ผู้จัดหา ผู้ให้บริการ ผู้รับทำงาน ที่ปรึกษา ผู้ประกอบวิชาชีพ พนักงาน เจ้าหน้าที่ ลูกจ้าง ตัวแทน และบุคคลใด ๆ ที่เกี่ยวข้องกับการดำเนินงาน การดำเนินธุรกิจและการดำเนินงานต่าง ๆ ของบริษัทฯ

**ผู้ควบคุมข้อมูลส่วนบุคคล** หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

**ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล** หมายถึง ผู้ที่ได้รับมอบหมายให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคล

**ผู้ประมวลผลข้อมูลส่วนบุคคล** หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล โดยบุคคลหรือนิติบุคคลดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

**คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล** หมายถึง ประธานคณะกรรมการ รองประธานคณะกรรมการ ซึ่งได้รับการประกาศแต่งตั้ง รวมถึงผู้จัดการทุกหน่วยงานซึ่งเป็นกรรมการโดยตำแหน่ง

**เจ้าหน้าที่ควบคุมข้อมูลส่วนบุคคล (DPO)** หมายถึง ผู้ที่บริษัทฯ แต่งตั้ง/มอบหมายเพื่อทำหน้าที่ให้คำแนะนำ หรือ ตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ ให้เป็นไปตามกฎหมาย

**การรั่วไหลของข้อมูลส่วนบุคคล** หมายถึง การรั่วไหล หรือการละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคล การส่งผ่านข้อมูลส่วนบุคคลจากภายในบริษัทฯ ไปยังภายนอกบริษัทฯ ทำให้เกิดความเสียหาย การถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น โดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล

**การละเมิดข้อมูลส่วนบุคคล** หมายถึง ข้อมูลส่วนบุคคลที่บริษัทฯ เก็บไว้อยู่ภายใต้การเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาตหรือสูญหาย

**NCB** หมายถึง บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

**ปปง.** หมายถึง สำนักงานป้องกันและปราบปรามการฟอกเงิน



## วัตถุประสงค์

คู่มือการปฏิบัติงานฉบับนี้จัดทำขึ้นเพื่อให้พนักงาน และบุคคลที่มีส่วนเกี่ยวข้องกับบริษัท ให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด บริษัทจึงมีแนวทางในการจะต้องปฏิบัติตามแนวทางการปฏิบัติงานภายในองค์กรตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ฉบับนี้จัดทำขึ้นภายใต้นโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทโดยมีวัตถุประสงค์ ดังนี้

1. เพื่อให้พนักงานหรือบุคคลที่เกี่ยวข้องจะได้ปฏิบัติงานของบริษัท เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. เพื่อเป็นแนวปฏิบัติในการบริหารจัดการได้แก่ การจัดเก็บ การรวบรวม การดูแลรักษาและการใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลอย่างชัดเจนและมีประสิทธิภาพ
3. เพื่อให้ลูกค้า คู่ค้า พันธมิตรทางธุรกิจ กรรมการบริษัทฯ ผู้บริหารและบุคลากรของบริษัทเกิดความเชื่อมั่นว่าข้อมูลส่วนบุคคลของท่านที่ได้ให้ไว้กับบริษัทได้รับการคุ้มครองและได้รับการป้องกันให้เกิดความเสี่ยงน้อยที่สุด



## 1. แนวทางปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล<sup>1</sup> บริษัทต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ ขอบเขตในการเก็บรวบรวม และจัดเก็บข้อมูลส่วนบุคคลเพียงพอที่จำเป็นแก่การให้บริการ การขอเข้าทำสัญญาและเป็นการจำเป็นตามกฎหมาย ซึ่งปกติพนักงานสาขาจะต้องขอข้อมูลส่วนบุคคลจากลูกค้า ซึ่งเป็นข้อมูลที่ สามารถระบุตัวตนของลูกค้าอันเป็นการจำเป็น เพื่อใช้เป็นข้อมูลประกอบการพิจารณาขอเข้าทำสัญญาและบริษัทอาจจัดเก็บข้อมูลส่วนบุคคลของลูกค้าเพิ่มเติม เพื่อประกอบการพิจารณาสินเชื่อเพิ่มเติม หรือเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่น หรือเก็บข้อมูลเนื่องจากมีวัตถุประสงค์ใหม่ ทั้งนี้ บริษัทจะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนทำการเก็บรวบรวม โดยอาจทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ก็ได้ ดังนั้น บริษัทจึงกำหนดแนวปฏิบัติที่ ชัดเจน เพื่อให้สามารถปฏิบัติได้อย่างถูกต้องครบถ้วน

นอกจากนี้ บริษัทต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพนักงาน เพื่อประโยชน์ในการบริหารจัดการทรัพยากรบุคคล ตามขั้นตอนการดำเนินการบริหาร ทรัพยากรบุคคล ตามกฎหมายที่เกี่ยวข้อง และตามนโยบายการบริหารจัดการของฝ่ายบริหารรวมถึงมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของบุคคลที่สามที่เกี่ยวข้องกับพนักงานหรือผู้สมัคร เพื่อประโยชน์ในการปฏิบัติ ตามข้อสัญญาและกฎหมายที่เกี่ยวข้องนั้น

1.2. การใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้กับบุคคล บริษัทในเครือ และหน่วยงานอื่น ๆ ต้องกำหนดให้ สอดคล้องกับกฎหมายนี้และกฎหมายอื่น โดยลูกค้า พนักงาน และบริษัทต้องรับทราบถึงวัตถุประสงค์ และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน ซึ่งบริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จะต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง

1.3. ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พนักงานต้องคำนึงถึง ความเป็นอิสระของเจ้าของ ข้อมูลส่วนบุคคล โดยจะต้องไม่มีเงื่อนไขในการให้ความยินยอม เพื่อเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการทำสัญญา และต้องให้สิทธิเจ้าของข้อมูล ถอนความยินยอมเมื่อใดก็ได้ โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอมและ ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลในเรื่องใด พนักงานต้องแจ้งให้เจ้าของ ข้อมูลทราบถึงผลกระทบจากการถอนความยินยอมนั้น<sup>2</sup>

1.4. ห้ามพนักงานทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจาก เจ้าของข้อมูลส่วนบุคคล การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สามารถกระทำได้เมื่อ

1.4.1 เพื่อการทำสัญญา<sup>3</sup>

1.4.2 การเก็บข้อมูลโดยมีวัตถุประสงค์ใหม่<sup>4</sup>

1.4.3 การเก็บรวบรวมข้อมูลจากแหล่งอื่น<sup>5</sup>

<sup>1</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27-29

<sup>2</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

<sup>3</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

<sup>4</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21

<sup>5</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25



1.4.4 การเก็บข้อมูลเพิ่มเติมซึ่งเป็นข้อมูลอ่อนไหว เพื่อประกอบการพิจารณาสินเชื่อ พนักงานต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน แต่มีบางกรณีที่พนักงานสามารถกระทำได้โดยไม่ต้องขอความยินยอมเพราะได้รับยกเว้น ด้วยเหตุ ดังต่อไปนี้

- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
- เมื่อเป็นการกระทำตามกฎหมาย เช่น ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน ประมวลกฎหมายแพ่งและอาญา ประมวลกฎหมายวิธีพิจารณาความแพ่งและอาญา พระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต กฎหมายว่าด้วยภาษีอากร กฎหมายว่าด้วยการประกอบธุรกิจประกันภัย พระราชบัญญัติประกันชีวิต พระราชบัญญัติคุ้มครองแรงงาน เป็นต้น
- เป็นไปเพื่อประโยชน์แก่การสอบสวนของพนักงานสอบสวน หรือการพิจารณาพิพากษาคดีของศาล<sup>6</sup>
- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ เพื่อประโยชน์สาธารณะ หรือเพื่อการศึกษา วิจัย การจัดทำสถิติ ซึ่งได้จัดให้มีมาตรการป้องกันที่เหมาะสม<sup>7</sup>
- เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล และการขอความยินยอมไม่อาจกระทำได้ในเวลานั้น<sup>8</sup>
- เป็นการจำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล<sup>9</sup>
- เป็นการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของบริษัท หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

1.5. บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อตรวจสอบดูแลประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ช่วยรักษาความปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลและปฏิบัติให้สอดคล้องกับกฎหมายนี้<sup>10</sup>

<sup>6</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4(5)

<sup>7</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(1)

<sup>8</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (2)

<sup>9</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (6)

<sup>10</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41





## 2. แนวทางปฏิบัติงานการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล

### 2.1. วัตถุประสงค์

เพื่อให้มีความสำคัญในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยให้พนักงานใช้เป็นคู่มือในการปฏิบัติงานเกี่ยวกับกระบวนการจัดการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล การจัดเก็บความยินยอมของเจ้าของข้อมูลส่วนบุคคล และการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้หน่วยงานประมวลผลตามวัตถุประสงค์ที่ได้แจ้งไว้รวมถึงการขอเพิกถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

### 2.2. ผู้รับผิดชอบ และหน้าที่ความรับผิดชอบ

บริษัทฯ มีหน้าที่ความรับผิดชอบ ดังนี้

1. แจ้งวัตถุประสงค์ของการจัดเก็บ ใช้งาน และการเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลทราบ
2. แจ้งวัตถุประสงค์ที่เพิ่มเติมหรือเปลี่ยนแปลงแก่เจ้าของข้อมูลส่วนบุคคลทราบ
3. ขอความยินยอมจากเจ้าของข้อมูล
4. ตรวจสอบการยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล หรือผู้มีอำนาจกระทำแทนเจ้าของข้อมูลส่วนบุคคล
5. จัดเก็บผลการยินยอมทั้งที่ยินยอมและปฏิเสธ

### 2.3. การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

#### 2.3.1. ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้<sup>11</sup>

บริษัทฯ สามารถจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่ได้รวบรวมไว้ก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้ไว้ได้ ซึ่งต้องดำเนินการภายใต้วัตถุประสงค์เดิมและจะต้องแจ้งวิธีการเพิกถอนความยินยอมให้เจ้าของข้อมูลที่ไม่ประสงค์ให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลรับทราบ

<sup>11</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 95



### 2.3.2. การขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลหลังที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้<sup>12</sup>

ขั้นตอน	รายละเอียด
1	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยืนยันตัวตน โดยใช้แนวปฏิบัติการยืนยันตัวตนตาม ข้อ 2.6 แนวปฏิบัติการยืนยันตัวตน
2	<b>เจ้าของข้อมูลส่วนบุคคล</b> แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> พิจารณาการยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ <ul style="list-style-type: none"><li>• กรณีผลการพิจารณายืนยันตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 4</li><li>• กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ</li></ul>
4	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> แจ้งวัตถุประสงค์ของการจัดเก็บ และการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลรับทราบ ผ่านช่องทางที่เหมาะสม และเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ แอปพลิเคชัน เอกสาร หรือป้ายประกาศต่างๆ เป็นต้น โดยหากมีการใช้ หรือประมวลผลข้อมูลส่วนบุคคล โดยบุคคลที่สามจะต้องมีการระบุรายละเอียดดังต่อไปนี้ <ul style="list-style-type: none"><li>• ข้อมูลส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่จะมีการใช้ร่วมกัน</li><li>• ระบุชื่อบุคคลที่สามที่ใช้ข้อมูลส่วนบุคคลร่วมกันให้ชัดเจน</li><li>• เหตุผลของการใช้ข้อมูลส่วนบุคคลร่วมกัน</li></ul>
5	<b>เจ้าของข้อมูลส่วนบุคคล</b> พิจารณาว่าจะให้ความยินยอมในการใช้ เปิดเผย หรือจัดเก็บ ตามวัตถุประสงค์ตามที่ บริษัทฯ แจ้งหรือไม่
6	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือไม่ยินยอม <ul style="list-style-type: none"><li>• <b>กรณียินยอม</b> : <b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ ที่ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับ ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li><li>• <b>กรณีไม่ยินยอม</b> : <b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li></ul>

<sup>12</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19



### 2.3.3. ขั้นตอนปฏิบัติงานต่อการเปิดเผยหรือเปลี่ยนแปลงวัตถุประสงค์ในการใช้งาน<sup>13</sup>

ขั้นตอน	รายละเอียด
1	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยืนยันตัวตน โดยใช้แนวปฏิบัติการยืนยันตัวตนตาม ข้อ 3.6 แนวปฏิบัติการยืนยันตัวตน
2	<b>เจ้าของข้อมูลส่วนบุคคล</b> แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> พิจารณาการยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ <ul style="list-style-type: none"><li>• กรณีผลการพิจารณายืนยันตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 4</li><li>• กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ</li></ul>
4	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> แจ้งประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ให้แก่เจ้าของข้อมูลส่วนบุคคลที่บริษัทฯ ได้จัดเก็บข้อมูลส่วนบุคคลไว้ให้ทราบผ่านช่องทางที่เหมาะสมและเจ้าของข้อมูลส่วนบุคคลเข้าถึงได้สะดวก เช่น บนเว็บไซต์ แอปพลิเคชัน เอกสารหรือป้ายประกาศต่างๆ เป็นต้น เมื่อมีการเปิดเผยหรือเปลี่ยนแปลงวัตถุประสงค์ในการใช้งาน
5	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> แจ้งวัตถุประสงค์ของการจัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่เพิ่มเติม หรือเปลี่ยนแปลงให้เจ้าของข้อมูลส่วนบุคคลรับทราบผ่านช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้สะดวก ตามที่ได้ระบุไว้ในขั้นตอนที่ 4 ในกรณีมีการใช้ หรือประมวลผลข้อมูลส่วนบุคคล โดยบุคคลที่สามจะต้องมีการระบุนรายละเอียดดังต่อไปนี้ <ul style="list-style-type: none"><li>• ข้อมูลส่วนตัวของเจ้าของส่วนบุคคลที่จะมีการใช้ร่วมกัน</li><li>• ระบุชื่อบุคคลที่สามที่ใช้ข้อมูลส่วนบุคคลร่วมกันให้ชัดเจน</li><li>• เหตุผลของการใช้ข้อมูลส่วนบุคคลร่วมกัน</li></ul>
6	<b>เจ้าของข้อมูลส่วนบุคคล</b> พิจารณาว่าจะให้ความยินยอมการจัดเก็บ หรือประมวลผลข้อมูลตามวัตถุประสงค์ที่บริษัทฯ แจ้งหรือไม่
7	<b>ผู้ควบคุมข้อมูลส่วนบุคคล</b> ทำการบันทึก และจัดเก็บเกี่ยวกับความยินยอม หรือไม่ยินยอม <ul style="list-style-type: none"><li>• <b>กรณียินยอม</b> : ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ ที่ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li><li>• <b>กรณีไม่ยินยอม</b> : ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกและ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสารตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li></ul>

<sup>13</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 และมาตรา 21



### 2.3.4. การขอความยินยอมผ่านคุกกี้ (Cookies)

ขั้นตอน	รายละเอียด
1	เจ้าของข้อมูลส่วนบุคคล เข้าสู่หน้าเว็บไซต์ของบริษัทฯ
2	ผู้ควบคุมข้อมูลส่วนบุคคล โดยเว็บไซต์ของบริษัทฯ แสดงแถบการยอมรับคุกกี้ (Cookie Consent Banner) ที่แจ้งวัตถุประสงค์การจัดเก็บ ใช้งานข้อมูลของคุกกี้ กรณีมีหลายวัตถุประสงค์จะต้องแยกความยินยอมเป็นรายวัตถุประสงค์ เพื่อให้เจ้าของข้อมูลส่วนบุคคลพิจารณายืนยันหรือปฏิเสธความยินยอมเป็นรายวัตถุประสงค์บนหน้าเว็บไซต์
3	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะยินยอมให้บริษัทฯ จัดเก็บใช้งานข้อมูลคุกกี้ในฐานะผู้ใช้งานหรือไม่
4	<p>ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือไม่ยินยอม</p> <ul style="list-style-type: none"><li>• <b>กรณียินยอม :</b> ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li><li>• <b>กรณีไม่ยินยอม :</b> ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคลที่ได้ให้ไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล</li><li>• <b>กรณีที่ไม่ได้ระบุความยินยอม :</b> ให้ระบบแจ้งวัตถุประสงค์การจัดเก็บการใช้งานข้อมูลคุกกี้อีกครั้ง</li></ul>



#### 2.4. ขั้นตอนปฏิบัติงานต่อการจัดเก็บความยินยอม

ขั้นตอน	รายละเอียด
1	จัดทำแบบฟอร์มการขอความยินยอมไว้ ตามประเภท ขอบเขต หรือตามที่ได้มีการปรับปรุงเนื้อหาในแบบฟอร์มดังกล่าว เพื่อไม่ให้กระทบฟอร์มเดิมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ผลการยินยอมไว้ และสามารถตรวจสอบ และเปรียบเทียบได้
2	บันทึกเนื้อหา และข้อมูล หลังเสร็จสิ้นกระบวนการการขอความยินยอม ดังนี้ <ul style="list-style-type: none"><li>• ชุดเนื้อหาข้อมูลการขอความยินยอม</li><li>• วิธีการให้ความยินยอม</li><li>• สถานะยินยอม หรือไม่ยินยอมตามรายการวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้แจ้งไว้</li><li>• แบบฟอร์มอิเล็กทรอนิกส์ที่ใช้บันทึก หรือแบบฟอร์มเอกสารที่เป็นกระดาษ</li></ul>
3	รวบรวมจัดเก็บความยินยอมที่ได้รับ ผ่านช่องทางต่าง ๆ ไว้ ณ ที่จัดเตรียมไว้ภายใต้มาตรการรักษาความปลอดภัยที่เพียงพอ ไม่ว่าจะ เป็นระบบอิเล็กทรอนิกส์ หรือแฟ้มเอกสารซึ่งเป็นกระดาษที่เก็บรักษาไว้ในสถานที่มั่นคงปลอดภัย
4	กำหนดการตรวจสอบ ทบทวน ความเหมาะสม และขอบเขตของความยินยอม ให้ทันสมัย และเป็นปัจจุบัน

#### 2.5. การขอเพิกถอนความยินยอมการใช้ เปิดเผยข้อมูลส่วนบุคคล

ขั้นตอน	รายละเอียด
1	บริษัทฯ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการดังนี้ <ul style="list-style-type: none"><li>• แจ้งเจ้าของข้อมูลส่วนบุคคลถึงสิทธิการขอเพิกถอนความยินยอมในการใช้ เปิดเผยข้อมูลส่วนบุคคล โดยสามารถกระทำได้ตลอดเวลา และง่ายต่อการเพิกถอนความยินยอม</li><li>• แจ้งขั้นตอนสำหรับการขอเพิกถอนความยินยอมดังกล่าว รวมถึงการอ้างอิงใด ๆ ต่อข้อผูกพันทางกฎหมาย หรือทางกฎหมายที่อาจยังคงมีผลบังคับใช้แม้หลังจากเจ้าของข้อมูลส่วนบุคคลได้ทำการเพิกถอนความยินยอม</li><li>• แจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบว่าการขอเพิกถอนความยินยอมดังกล่าว จะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลได้</li></ul>
2	เมื่อเจ้าของข้อมูลส่วนบุคคลแสดงความประสงค์การขอเพิกถอนความยินยอม ให้ปฏิบัติตามขั้นตอนปฏิบัติงานการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
3	ให้กำหนดวิธีการในการขอเพิกถอนความยินยอม โดยใช้ช่องทาง และรูปแบบเดียวกันกับเมื่อตอนแสดงการร้องขอความยินยอม เพื่อให้กระบวนการสอดคล้องกันและสามารถตรวจสอบได้



## 2.6. การปฏิบัติการยืนยันตัวตน

กำหนดแนวปฏิบัติการยืนยันตัวตน โดยเจ้าของข้อมูลส่วนบุคคลต้องดำเนินการยืนยันตัวตนให้ถูกต้องอย่างน้อย 3 รายการแรก ดังนี้

1. ชื่อ
2. นามสกุล
3. เลขบัตรประจำตัวประชาชน
4. วัน เดือน ปี เกิด
5. ที่อยู่
6. หมายเลขโทรศัพท์
7. อีเมล
8. ความสัมพันธ์กับบริษัทฯ เช่น ลูกค้า ผู้สมัครงาน พนักงาน ครอบครัวของพนักงาน ผู้ใช้งานหรือเข้าชมเว็บไซต์ เป็นต้น



### 3. แนวทางปฏิบัติในการเก็บรวบรวมข้อมูลส่วนบุคคล

#### 3.1. การควบคุมการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้ำก่อนเข้าทำสัญญา

พนักงานสาขาต้องมีการเก็บรวบรวมข้อมูลของลูกค้าเพื่อการทำกรยืนยันตัวตน การส่งข้อมูลตรวจสอบกับ NCB และตรวจสอบตามกฎหมาย ป.ง. หรือกฎหมายอื่น ซึ่งมีความจำเป็นต้องขอข้อมูลส่วนบุคคลก่อนการพิจารณาเข้าทำสัญญากับบริษัท ดังนั้น บริษัทจึงกำหนดให้มีแบบฟอร์ม 3 ฉบับ ได้แก่

##### 3.1.1. เอกสารประกอบการทำสัญญา

##### 3.1.2. หนังสือให้ความยินยอมตรวจสอบข้อมูลเครดิต

##### 3.1.3. หนังสือให้ความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยมีรายละเอียดในหนังสือให้ความยินยอม ดังนี้<sup>14</sup>

- แจ้งวัตถุประสงค์ในการรวบรวม ใช้ หรือเปิดเผยข้อมูล
- ระบุว่าบริษัทอาจต้องเปิดเผยข้อมูลส่วนใดบ้าง เพื่อวัตถุประสงค์อะไร
- ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล
- แจ้งสิทธิและวิธีการเข้าถึงข้อมูลฯ ให้เจ้าของข้อมูลทราบ และการถอนความ ยินยอม
- ข้อมูลการติดต่อและวิธีการติดต่อตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- มีการบันทึกรายงานการปฏิเสธคำขอเข้าถึงข้อมูล ขอสำเนา ขอแก้ไขข้อมูลหรือการคัดค้านการรวบรวม ใช้ หรือเปิดเผยข้อมูล เพื่อให้สำนักงานและเจ้าของข้อมูลตรวจสอบได้<sup>15</sup>
- ในการให้ความยินยอมจะคำนึงถึงความเป็นอิสระกับเจ้าของข้อมูลส่วนบุคคล ข้อความชัดเจน ไม่กำกวม ไม่เป็นการหลอกลวง ทั้งนี้ในการเข้าทำสัญญา รวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอม เพื่อเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่ไม่มีความจำเป็น หรือที่เกี่ยวข้อง สำหรับการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการนั้น ๆ

#### 3.2. การเก็บรวบรวมข้อมูลเพิ่มเติม และเก็บรวบรวมข้อมูลจากแหล่งอื่น<sup>16</sup>

3.2.1. การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น เพื่อประกอบการพิจารณาอนุมัติสินเชื่อของฝ่ายพนักงานสาขาหรือผู้มีอำนาจอนุมัติ เนื่องจากบริษัทได้มีการจัดทำหนังสือเพื่อขอความยินยอมจากลูกค้ำ ซึ่งถือเป็นการแจ้งให้ทราบล่วงหน้าเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจาก แหล่งอื่น เพื่อการตรวจสอบ ยืนยันข้อมูลให้ถูกต้อง เป็นการรักษาสีทธิตามกฎหมาย ของบริษัท ซึ่งหากทางบริษัทหรือหน่วยงานนั้น ๆ ปฏิเสธการให้ข้อมูล บริษัทสามารถแสดงหนังสือยินยอมในการขอตรวจสอบยืนยันข้อมูลได้

<sup>14</sup> แบบฟอร์มตามเอกสารแนบท้าย 6

<sup>15</sup> แบบฟอร์มตามเอกสารแนบท้าย 4

<sup>16</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25



- 3.2.2. หากมีข้อมูลที่ต้องเก็บรวบรวมเพิ่มเติม เพื่อการวิเคราะห์สินเชื่อ และการติดตามเรงรัดหนี้สิน สามารถตรวจสอบติดตามข้อมูลใน Facebook หรือสื่อ Social อื่น ที่แจ้งไว้เป็นสาธารณะได้โดยไม่ต้องขอความยินยอม<sup>17</sup>
- 3.2.3. การตรวจสอบข้อมูลโดยการคัดแบบริ่องรายการทะเบียนราษฎร เนื่องจากการผิदनัดชำระหนี้ เพื่อใช้เป็นข้อมูลในการส่งหนังสือบอกกล่าวทวงถามนั้น สามารถทำได้ตามที่กฎหมายกำหนดไว้ ไม่ต้องแจ้งหรือขอความยินยอมก่อน
- 3.2.4. การไปตรวจสอบที่อยู่ บ้านหรือบริษัท เพื่อประกอบการประเมินวิเคราะห์การออกสินเชื่อ สามารถทำได้และได้แจ้งให้ลูกค้าเจ้าของข้อมูลทราบแล้ว โดยจากการเขียนแผนที่บ้านหรือบริษัทและลงนามในหนังสือให้ความยินยอมแล้ว

### 3.3. การกำหนดและแยกแยะข้อมูลส่วนบุคคล

- 3.3.1. หลังจากมีการเก็บรวบรวมข้อมูลมาแล้วนั้น บริษัทจะทำการจัดเก็บและคัดแยกข้อมูลส่วนบุคคลตามขอบเขตของข้อมูลส่วนบุคคล ดังนี้
  - การแยกแยะข้อมูลที่สามารถระบุตัวบุคคลออกจากกันได้ “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่ระบุไปถึง “เจ้าของข้อมูล” ได้โดยเจ้าของ ข้อมูลนั้นอาจเป็นบุคคลหรือนิติบุคคลก็ได้ ก่อนการใช้และเปิดเผยจึงต้องมีการ แยกแยะว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลและข้อมูลใดที่ไม่เป็นข้อมูลส่วนบุคคล มี รายละเอียด ดังนี้

#### ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคล

- (1) ชื่อ - นามสกุล หรือชื่อเล่น
- (2) เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)
- (3) ที่อยู่, อีเมลล์, เบอร์โทรศัพท์
- (4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID
- (5) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, फिल्मเอกซเรย์, ข้อมูลสแกนตาม ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม
- (6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน, ทะเบียนบ้าน
- (7) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่, ข้อมูลการแพทย์, ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน
- (8) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
- (9) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file
- (10) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

<sup>17</sup> ได้รับการยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26(3)





### ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

- (1) เลขทะเบียนบริษัท
- (2) ข้อมูลสำหรับการติดต่อธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือแฟกซ์ที่ทำงาน ที่อยู่สำนักงาน, อีเมลที่ใช้ในการทำงาน, อีเมลของบริษัท เช่น XXX@nimleasing.com เป็นต้น
- (3) ข้อมูลนิรนาม (Anonymized Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึงข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถ ระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค
- (4) ข้อมูลผู้ตาย

#### 3.3.2. การติดตามพฤติกรรมหรือกิจกรรมของบุคคล

การที่ข้อมูลสามารถถูกใช้ในการติดตามพฤติกรรมหรือกิจกรรมที่บุคคลนั้นทำได้ เช่น log file โดยการเก็บ log file คือสิ่งที่ต้องทำสำหรับบริษัท เช่น การใช้งาน e-mail ในบริษัท การใช้งาน อินเทอร์เน็ตของพนักงาน เป็นต้น ทั้งนี้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ เพื่อแยกแยะ ไม่ว่าจะผู้ใช้งานคือใคร มีพฤติกรรมการใช้งานอย่างไร สามารถ ตรวจสอบได้และเป็นหลักฐานประกอบการทำงาน ได้อย่างมีประสิทธิภาพ

#### 3.3.3. การเชื่อมโยง

การที่ข้อมูลสามารถถูกใช้เชื่อมโยงกัน เพื่อระบุไปถึงตัวบุคคลได้ โดยแบ่งออกเป็น 2 กรณี คือ

1. ข้อมูลที่ถูกเชื่อมโยงแล้ว เป็นกรณีหากมีข้อมูลที่เกี่ยวข้องกับข้อมูลที่ใช้ร่วมกัน แล้วสามารถระบุถึงตัวบุคคล เช่น ชุดข้อมูล 2 ชุด แต่ละชุดมีข้อมูล แยกกัน แต่หากมีบุคคลที่สามารถเข้าถึงข้อมูลทั้ง 2 ชุดนั้นได้ก็จะสามารถ เชื่อมโยงและระบุไปถึงตัวบุคคลได้

2. ข้อมูลที่อาจถูกเชื่อมโยง เป็นกรณีหากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูล อื่นแล้ว ก็จะสามารถระบุตัวบุคคลได้ แต่โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมกัน นั้นไม่อยู่ในระบบ หรืออยู่ในอินเทอร์เน็ต หรืออยู่ที่อื่นใด หมายเหตุ แม้ว่าข้อมูลนั้นจะไม่สามารถใช้ระบุถึงตัวบุคคลได้ แต่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่น ๆ ประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ โดยไม่จำเป็นว่าข้อมูลหรือ สารสนเทศอื่นนั้นได้มีอยู่ด้วยกัน

#### 3.3.4. ข้อมูลอ่อนไหว

เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้จริง แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ซึ่งบริษัทต้องมีการเก็บรวบรวมข้อมูล เชื้อชาติ ศาสนา ข้อมูลสุขภาพ จากลูกค้า ในการขอเข้าทำสัญญา เพื่อประกอบการวิเคราะห์สินเชื่อ โดยมีการส่งข้อมูลให้กับหน่วยงานที่เกี่ยวข้องด้วย หากบริษัทมีความจำเป็นที่จะต้องเก็บข้อมูลประเภทนี้ จะต้องมีการขอความยินยอมจากลูกค้าในเรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ก่อนด้วยทุกครั้ง ข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพร่างกาย หรือข้อมูลสุขภาพจิต ข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชน



### 3.3.5. ข้อมูลแฝง

เป็นข้อมูลส่วนบุคคลที่ถูกแฝงข้อมูลที่ระบุตัวบุคคลได้เอาไว้ โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคลด้วยข้อมูลอื่น หรือเลขที่กำหนดขึ้นมา โดยที่ข้อมูลที่เกี่ยวข้องอื่น ๆ

- ไม่เพียงพอที่จะสามารถเชื่อมโยงกลับไปยังเจ้าของข้อมูลได้ หรือ
- กรณีที่ผู้เชี่ยวชาญโดยทั่วไปแม้จะได้ใช้ความพยายามตามสมควรแล้ว ก็ไม่สามารถใช้กระบวนการใด ๆ เพื่อเชื่อมโยงกลับไปยังตัวเจ้าของข้อมูลได้ เว้นแต่ตัวผู้ทำการแฝงข้อมูลดำเนินการเอง

#### **สรุปแนวทางปฏิบัติในการเก็บรวบรวมข้อมูลส่วนบุคคล**

1. แต่ละฝ่ายในบริษัทต้องเก็บรวบรวมข้อมูลส่วนบุคคล ภายใต้นโยบายนี้และมีการให้เจ้าของข้อมูลส่วนบุคคลลงนามในหนังสือให้ความยินยอมและยอมรับนโยบายคุ้มครองข้อมูลส่วนบุคคล
2. การกำหนดและแยกแยะข้อมูลเพื่อจัดเก็บ ใช้ หรือเปิดเผย ให้เป็นไปตามรายละเอียดใน **ข้อ 3.3 การกำหนดและแยกแยะข้อมูลส่วนบุคคล** โดยเมื่อเก็บรวบรวมข้อมูลมาแล้ว ให้จัดเก็บไว้ในที่เหมาะสมปลอดภัย ที่บริษัทกำหนดไว้ตามระเบียบการปฏิบัติงานของแต่ละหน่วยงาน และปฏิบัติตามแนวทางปฏิบัติในการการใช้และเปิดเผยข้อมูลในข้อต่อไปที่ได้อธิบายไว้แล้ว
3. หน่วยงานที่เก็บรวบรวมข้อมูลส่วนบุคคล

#### 3.1. สำนักงานสาขา

สาขาต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าในการเข้าทำสัญญา โดยข้อมูลที่ต้องมีการเก็บรวบรวม ได้แก่ ข้อมูลส่วนบุคคลทั่วไป (ชื่อ-สกุล, เลขบัตรประชาชน, เลขบัญชีธนาคาร, ที่อยู่ : อีเมล, เบอร์โทรศัพท์) เป็นต้น ข้อมูลข้างต้นเป็นข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่มีความจำเป็นต้องเก็บรวบรวมเพื่อใช้ในการเข้าทำสัญญา และตามกฎหมายของ NCB กับปบง. ให้เก็บรวบรวมข้อมูลดังกล่าวได้ ตามมาตรา 4 (2) และ (6) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยเอกสารที่พนักงานสาขาต้องเสนอให้ลูกค้าลงลายมือชื่ออันมีรายละเอียดตามข้อ 2.1 การควบคุมการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าก่อนเข้าทำสัญญา ดังนั้นเอกสารประกอบที่ลูกค้านำส่งข้อมูลต่าง ๆ ของลูกค้า เมื่อไม่ได้มีการใช้งานแล้ว ให้พนักงานสาขาทำการทำลายด้วยเครื่องทำลายเอกสาร หรือวิธีการอื่นใดที่ทำให้ไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ และ ไม่นำมาเป็นกระดาษรีไซเคิล (Recycle) เพื่อความปลอดภัยของข้อมูลลูกค้า หากยังคงต้องใช้งานให้จัดเก็บไว้ในตู้เอกสารหรือในไฟล์กลางของบริษัทที่มีการเข้ารหัสไว้

เมื่อได้รับเอกสารจากลูกค้า พนักงานสาขาจะต้องตรวจสอบความถูกต้องครบถ้วนของข้อมูลและเอกสารก่อนบันทึกข้อมูลลงในระบบ หากมีข้อมูลไม่ครบถ้วน ไม่ถูกต้องจะต้องทำการขอจากลูกค้าเจ้าของข้อมูลเพิ่มเติม นอกจากนี้โดยปกติจะมีการเก็บข้อมูลลูกค้าไว้ในรูปแบบไฟล์อิเล็กทรอนิกส์ในฐานะระบบบริษัท ซึ่งมีการตั้งเข้ารหัสและจำกัดสิทธิการเข้าถึงตามตำแหน่งและหน้าที่ด้วยแล้ว ดังนั้น ข้อมูลในระบบจะต้องจัดเก็บในระบบ Server ที่มี



การรักษาความปลอดภัย มีรหัสการเข้าใช้งานหรือจำกัดสิทธิ์การเข้าดูตามตำแหน่งหน้าที่ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ตัวอย่างเอกสารที่มีการจัดเก็บของบริษัท ที่ต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เมื่อทำการถ่ายสำเนาบัตรประจำตัวประชาชนและสำเนาทะเบียนบ้านพนักงานต้องทำการขีดฆ่า ศาสนา กรุ๊ปเลือด (ถ้ามี) ทุกครั้งก่อนทำการเก็บ รวบรวมข้อมูลและเอกสาร



ตัวอย่างการขีดฆ่าบัตรประจำตัวประชาชนของเจ้าของข้อมูลส่วนบุคคล

- 3.2. ฝ่ายจัดการข้อมูลเครดิตบูโร เพื่อตรวจประเมินความเสี่ยงของลูกค้าแต่ละราย พนักงานจะทำการบันทึกข้อมูลเข้าระบบ NCB และรอข้อมูลที่ได้จาก NCB เพื่อนำมาประเมินวงเงินสินเชื่อ ดังนั้น หนังสือยินยอมการเปิดเผยข้อมูล NCB และเอกสารประกอบอื่นใด ที่ไม่ได้ใช้งานหรือเสร็จสิ้นกระบวนการใช้งานแล้ว ให้ทำลายโดยวิธีการอื่นใดที่เอกสารดังกล่าวไม่สามารถนำมาใช้ระบุตัวตนของเจ้าของข้อมูลได้ เพื่อความปลอดภัยของข้อมูลลูกค้า
- 3.3. ฝ่ายตรวจสอบ/การโอนเงิน
- 3.4. ฝ่ายทะเบียนธุรกรรม
- 3.5. ฝ่ายเร่งรัดหนี้สิน
- 3.6. เจ้าหน้าที่เฉพาะกิจ
- 3.7. ฝ่ายกฎหมาย

ฝ่ายกฎหมายจะดำเนินการตามขั้นตอนออกหนังสือบอกกล่าวทวงถามให้กับลูกค้าที่มีการผิดนัดชำระหนี้ ซึ่งฝ่ายกฎหมายจะสามารถดูข้อมูลส่วนบุคคลเกี่ยวกับลูกค้าได้ทั้งหมด และสามารถดำเนินการขอคัดสำเนาข้อมูลเพิ่มเติมจากหน่วยงานของรัฐได้ตามกฎหมายนี้ และกฎหมายอื่นที่เกี่ยวข้อง สามารถติดต่อขอข้อมูลเพิ่มเติมกับเจ้าของข้อมูลได้เท่าที่จำเป็นในการติดตามทรัพย์สินที่เป็นหลักประกัน นอกจากนี้มีการส่งข้อมูลให้กับหน่วยงานภายนอกหลายหน่วยงาน



### 3.8. ฝ่ายบริหารงานทั่วไป

เจ้าหน้าที่ฝ่ายบริหารงานทั่วไปจะเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานทุกคนในบริษัทและผู้สมัครทุกคน ซึ่งมีความจำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลทั้งข้อมูลทั่วไปและข้อมูลอ่อนไหว เช่น ชื่อ-สกุล ประวัติส่วนตัวด้าน การศึกษา การทำงาน ข้อมูลสุขภาพกายและสุขภาพจิต ศาสนา เชื้อชาติ ทศนคติและความเชื่อต่าง ๆ ซึ่งมีผลในการพิจารณาจ้างงาน และต้องมีการรายงานข้อมูลให้หน่วยงานที่เกี่ยวข้อง ได้แก่ สำนักงานประกันสังคม บริษัทประกัน เพื่อการคุ้มครองด้านสุขภาพและชีวิต ทั้งนี้ ได้มีการจัดเก็บเอกสารและข้อมูลส่วนบุคคลไว้ในที่ปลอดภัย มีมาตรการคุ้มครองความปลอดภัยตามระเบียบการดำเนินงานของฝ่ายบริหารงานทั่วไป

### 3.9. ฝ่ายพัฒนาระบบและเทคโนโลยีสารสนเทศ

### 3.10. ฝ่ายการตลาด

## 4. แนวทางปฏิบัติในการใช้และเปิดเผยข้อมูลส่วนบุคคล

ผู้เกี่ยวข้องกับข้อมูลส่วนบุคคล มี 4 ประเภท ดังนี้

- เจ้าของข้อมูลส่วนบุคคล
- ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูล
- บุคคลภายนอก (Third Parties)
  - เจ้าของข้อมูล (ลูกค้า พนักงาน) ส่งข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูล (บริษัท) เช่น เมื่อมีขอเข้าทำสัญญา ขอใช้บริการต่าง ๆ ของผู้ควบคุมข้อมูล (บริษัท) หรือทำสัญญาเป็นพนักงานของบริษัท เป็นต้น
  - ผู้ควบคุมข้อมูล (บริษัท) ส่งข้อมูลส่วนบุคคลของลูกค้าให้กับผู้ประมวลผลข้อมูล (Outsource) เช่น ตามข้อตกลงจ้างงานภายนอก (Outsourcing) เป็นต้น
  - เจ้าของข้อมูล (ลูกค้า พนักงาน) ส่งข้อมูลส่วนบุคคลให้กับผู้ประมวลผลข้อมูล (Outsource คู่ค้า) โดยตรง ซึ่งเป็นส่วนหนึ่งของการดำเนินงานในนามของผู้ควบคุมข้อมูล (บริษัท)
  - ผู้ควบคุมข้อมูล (บริษัท) ส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น การดำเนินการตามที่เจ้าของข้อมูลร้องขอ เป็นต้น
  - ผู้ประมวลผลข้อมูล (Outsource คู่ค้า) ส่งข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูล เช่น ตามที่ผู้ควบคุมสั่งการ เป็นต้น

### 4.1 การใช้และการเปิดเผยข้อมูลส่วนบุคคล

4.1.1. ให้พนักงานใช้และเปิดเผยข้อมูลส่วนบุคคลของลูกค้าตามความยินยอมของลูกค้าที่เป็นการใช้ตามวัตถุประสงค์ของการเก็บรวบรวม จัดเก็บข้อมูลของบริษัทเท่านั้น บริษัทจะกำกับดูแลพนักงาน เจ้าหน้าที่หรือผู้ปฏิบัติงานของบริษัทมิให้ใช้และ/หรือเปิดเผย ข้อมูลส่วนบุคคลของลูกค้านอกเหนือไปจากวัตถุประสงค์ที่ได้แจ้งและขอความยินยอมไว้ในการเก็บรวบรวมข้อมูลส่วนบุคคลหรือเปิดเผยต่อบุคคลภายนอก เว้นแต่ เป็นกรณีที่กฎหมาย



กำหนด หรือได้รับความยินยอมจากลูกค้าแล้ว หรือเป็นไปเพื่อประโยชน์เกี่ยวกับชีวิต สุขภาพ หรือความปลอดภัยของเจ้าของข้อมูล (ลูกค้า) หรือบุคคลอื่น หรือเพื่อประโยชน์ แก่การสอบสวนของพนักงานสอบสวน หรือการพิจารณาพิพากษาคดีของศาลหรือเพื่อ ประโยชน์ในการศึกษา วิจัย หรือจัดทำสถิติ

- 4.1.2. ในกรณีที่บริษัทต้องเปิดเผยข้อมูลให้กับบุคคลผู้รับจ้างงานของบริษัท บริษัทในเครือ หรือ ให้กับที่ปรึกษา บริษัทจะแจ้งและขอความยินยอมจากเจ้าของข้อมูลก่อน ทั้งนี้ บริษัทได้มี รายละเอียดในหนังสือยินยอมในการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการดำเนินงาน และสามารถทำได้ตามกฎหมายนี้ หรือกฎหมายอื่น
- 4.1.3. การส่ง โอน หรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลหรือบริษัทในเครือ ที่ปรึกษา ผู้รับ จ้าง บริษัทสามารถทำได้เมื่อขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นหนังสือหรือ โดยระบบอิเล็กทรอนิกส์ และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนซึ่ง บริษัทในเครือ ที่ปรึกษา และผู้รับจ้างนั้น จะต้องมีการรักษาความมั่นคงปลอดภัย โดยห้ามดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือจากที่บริษัทฯ กำหนด
- 4.1.4. การเปิดเผย หรือให้สิทธิการเข้าถึงข้อมูลกับหน่วยงานของรัฐตามกฎหมายนี้ และกฎหมาย อื่นสามารถทำได้โดยไม่ต้องขอความยินยอม เช่น ปปง. ศาล กรมสรรพากร เป็นต้น

#### 4.2. การควบคุมการใช้งานและการเข้าถึงข้อมูลส่วนบุคคล

- 4.2.1. พนักงาน บริษัทในเครือ ที่ปรึกษา และผู้รับจ้าง จะสามารถเข้าถึงข้อมูลหรือรับทราบ ข้อมูลตามความจำเป็นต่อการใช้ในการปฏิบัติงานเท่านั้น ไม่อนุญาตให้กำหนดสิทธิเกิน ความจำเป็นในการใช้งาน โดยฝ่ายเทคโนโลยีสารสนเทศและฝ่ายวางแผนและพัฒนา ระบบจะควบคุมการเห็นหรือใช้ ข้อมูลบนข้อมูลส่วนกลางของแต่ละหน่วยงานตามความ เหมาะสมนั้น
- 4.2.2. บริษัทได้จัดให้มีการบริหารจัดการสิทธิในการเข้าถึงข้อมูล มีบัญชีรายชื่อ กำหนดรหัสผ่าน ประจำตัวของพนักงานทุกคน เพื่อป้องกันการจำกัดสิทธิและการตรวจสอบ มีการกำหนด ระดับชั้นข้อมูลความลับ ซึ่งเป็นมาตรการความปลอดภัย ด้านข้อมูลที่บริษัทฯ กำหนดไว้ ตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยและเทคโนโลยีสารสนเทศและ ระเบียบว่าด้วยการรักษาข้อมูลส่วนบุคคลส่วนบุคคล
- 4.2.3. ในการใช้งานและเข้าถึงข้อมูลส่วนบุคคลนั้นจะเป็นไปตามวัตถุประสงค์ที่แจ้งกับลูกค้า พนักงาน จะไม่มีการใช้งานนอกวัตถุประสงค์นอกเหนือจากที่แจ้งลูกค้าไว้ ทั้งนี้ เจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคลจะเป็นผู้ตรวจสอบการดำเนินงาน และการใช้ข้อมูลนั้น

#### 4.3. การใช้หรือเปิดเผยข้อมูลส่วนบุคคลของแต่ละหน่วยงาน

- 4.3.1. ฝ่ายการตลาด มีการใช้และเปิดเผยข้อมูลส่วนบุคคล โดยส่วนใหญ่เฉพาะในบริษัท ระหว่างแผนก และมีการเก็บรวบรวมเพื่อทำสถิติ ปรับเปลี่ยนกลยุทธ์ทางการตลาดให้มีความเหมาะสม



- 4.3.2. ฝ่ายจัดการข้อมูลเครดิตบูโร มีการใช้และเปิดเผยข้อมูลให้กับ NCB ซึ่งเป็นการปฏิบัติงานตามหน้าที่ของเจ้าหน้าที่เครดิตบูโรที่บริษัทแต่งตั้งขึ้น และดำเนินการตาม พระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 และกฎหมายอื่นที่เกี่ยวข้อง รวมถึงธนาคารแห่งประเทศไทย(ธปท)และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)
- 4.3.3. ฝ่ายทะเบียนธุรกรรม มีการใช้และเปิดเผยข้อมูลส่วนบุคคลให้กับกรมขนส่งทางบกในการดำเนินงานที่เกี่ยวกับเล่มทะเบียนรถทั้งหมด
- 4.3.4. ฝ่ายบัญชีกลาง มีการใช้และเปิดเผยข้อมูลให้กับกรมสรรพากร เรื่อง ภาษี ตามประมวลกฎหมายภาษีอากร และอื่น ๆ ที่เกี่ยวข้อง มีการจัดส่งข้อมูลให้กับลูกค้า โดยจัดส่งผ่าน Outsource ได้แก่ ใบเสร็จรับเงิน ใบกำกับภาษี เอกสารการต่อภาษี เป็นต้น
- 4.3.5. ฝ่ายติดตามเร่งรัด
- 4.3.6. ฝ่ายกฎหมาย มีการใช้ข้อมูลกับหน่วยงาน ภายนอก งานฟ้องคดี งานบังคับคดี  
นอกจากนี้ บางกรณีอาจมีการดำเนินการส่งข้อมูลรายงานปง. ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 หรือหน่วยงานราชการอื่น ซึ่งเป็นการปฏิบัติตามกฎหมายสามารถกระทำได้  
บริษัทอาจมีการขายหนี้เสียบางส่วนออกไป โดยบริษัทที่จะรับซื้อหนี้ต้องมีข้อตกลงร่วมกับบริษัทในการรักษาข้อมูลความลับของลูกค้า ทั้งนี้เมื่อมีการขายหนี้ไปแล้วหมายถึงการโอนสิทธิในการเป็นเจ้าของหนี้ และหมายความว่าการควบคุมดูแลข้อมูลส่วนบุคคลของบริษัทที่รับซื้อหนี้ไปย่อมเป็นไปโดยต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่เป็นการบังคับใช้โดยทั่วไป
- 4.3.7. ฝ่ายบริหารงานทั่วไป มีการใช้และเปิดเผยข้อมูลส่วนบุคคลของพนักงาน ในการดำเนินการตามพระราชบัญญัติคุ้มครองแรงงาน พ.ศ.2541 และกฎหมายอื่นที่เกี่ยวข้อง และจำเป็นต้องมีการตรวจสอบประวัติอาชญากรรม ทั้งนี้ จะต้องมีการแจ้งให้พนักงานทราบและให้ความยินยอมเป็นหนังสือทุกครั้ง จึงจะสามารถดำเนินการได้
- 4.3.8. เจ้าหน้าที่เฉพาะกิจ มีการใช้และเปิดเผยข้อมูลของลูกค้าในการติดตามทวงถามกับบุคคลอ้างอิงที่ลูกค้าระบุไว้ในสัญญาว่าให้ดำเนินการติดตามทวงถามหนี้ได้



## 5. แนวทางปฏิบัติในการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

เพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานเกี่ยวกับกระบวนการรับแบบคำร้องการจัดการสิทธิคำร้อง รวมถึงการแจ้งใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

### 5.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล

5.1.1. สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามแนวปฏิบัตินี้ ได้แก่

1. สิทธิการได้รับแจ้งรายละเอียดข้อมูลในการเก็บรวบรวมข้อมูลส่วนบุคคล
2. สิทธิในการเพิกถอนความยินยอม
3. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
4. สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
5. สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
6. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล
7. สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล
8. สิทธิในการขอให้ระงับประมวลผลข้อมูลส่วนบุคคล

### 5.2 ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

ลำดับ	รายละเอียด	หน้าที่ความรับผิดชอบ
1	พนักงานผู้รับเรื่อง	<ol style="list-style-type: none"><li>1. รับคำร้องขอของเจ้าของข้อมูล</li><li>2. ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ</li></ol>
2	พนักงานคุ้มครองข้อมูลส่วนบุคคล	<ol style="list-style-type: none"><li>1. พิจารณาความถูกต้องของคำร้องขอ</li><li>2. พิจารณาค่าใช้จ่ายดำเนินการเพื่อปฏิบัติตามคำร้องขอ (ถ้าจำเป็น)</li><li>3. แจ้งผลการขอใช้สิทธิ</li><li>4. บันทึกผลการใช้หรือปฏิเสธการใช้สิทธิ</li></ol>
3	ผู้ควบคุมข้อมูลส่วนบุคคล	ดำเนินการหรือไม่ดำเนินการตามคำร้อง



### 5.3 ขั้นตอนปฏิบัติงานต่อการแจ้งใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล<sup>18</sup>

จะต้องดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคล โดยผู้รับผิดชอบดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า ภายใน 30 วัน นับแต่ที่ได้รับคำขอ

ขั้นตอน	รายละเอียด
1	เจ้าของข้อมูลส่วนบุคคล ผู้ร้องขอแจ้ง หรือผู้ยื่นคำร้องขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคล ผ่านทางช่องทางที่บริษัทฯ กำหนดไว้ช่องทางการติดต่อสอบถามหรือยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
2	พนักงานผู้รับเรื่อง ให้ดำเนินการดังต่อไปนี้ 2.1 รับคำขอจากเจ้าของข้อมูลส่วนบุคคล หรือผู้ยื่นคำร้องขอ ตามแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) 2.2 บันทึกรายละเอียดในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่
3	พนักงานผู้รับเรื่อง แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลหรือผู้ยื่นคำร้องทำการยืนยันตัวตน
4	พนักงานผู้รับเรื่อง พิจารณายืนยันตัวตน โดยใช้แนวปฏิบัติการยืนยันตัวตนตาม ข้อ 4.7 แนวปฏิบัติการยืนยันตัวตน 4.1 กรณียืนยันตัวตนไม่สำเร็จ : พนักงานผู้รับเรื่อง แจ้งผลยืนยันตัวตนของผู้ยื่นคำร้องขอใช้สิทธิไม่สำเร็จให้กับเจ้าของข้อมูลส่วนบุคคล และให้ถือว่าสิ้นสุดกระบวนการ 4.2 กรณียืนยันตัวตนสำเร็จ : ให้ดำเนินการขั้นตอนที่ 5 ต่อไป
5	พนักงานผู้รับเรื่อง ตรวจสอบหลักฐานแล้ว พบว่า 6.1 กรณีหลักฐานไม่ถูกต้อง ให้แจ้งผู้ยื่นคำร้องขอทราบ และให้ถือว่าสิ้นสุดกระบวนการ 6.2 กรณีหลักฐานถูกต้อง ให้ส่งเรื่องให้ส่วนงานที่เกี่ยวข้อง เพื่อพิจารณาคำร้องในขั้นตอนที่ 6 ต่อไป
6	DPO พิจารณาคำร้องขอของเจ้าของข้อมูลส่วนบุคคลว่าถูกต้อง สมบูรณ์ หรือเป็นคำขอที่สมเหตุสมผลหรือไม่ หรือมีเหตุแห่งการปฏิเสธคำร้องขอ นั้น ตาม ข้อ 5.4 เหตุแห่งการปฏิเสธ การปฏิบัติตามคำร้องขอของเจ้าของข้อมูล หรือไม่ 6.1 กรณี ไม่สามารถดำเนินการได้ตามคำร้องขอ ให้ดำเนินการดังต่อไปนี้ 6.1.1 DPO แจ้งเหตุผลการปฏิเสธคำร้องขอแก่เจ้าของข้อมูลส่วนบุคคลตาม หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding) 6.1.2 DPO บันทึกเหตุผลการปฏิเสธการปฏิบัติตามคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลลงในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ 6.1.3 สิ้นสุดกระบวนการ 6.2 กรณี สามารถดำเนินการได้ตามคำร้องขอ ให้ดำเนินการตามขั้นตอนที่ 7 ต่อไป

<sup>18</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30, 32, 33, 34, 35, 36, 37, 73





ขั้นตอน	รายละเอียด
7	<p>DPO พิจารณาค่าใช้จ่ายกรณีที่มีการขอในรูปแบบเอกสารเป็นจำนวนมากต่อคำร้องขอนั้น</p> <p>7.1 <b>กรณีที่ไม่มีค่าใช้จ่าย</b> ให้ดำเนินการดังต่อไปนี้</p> <p>7.1.1 DPO ดำเนินการแจ้งให้ผู้ที่เกี่ยวข้อง ดำเนินการตามคำขอ</p> <p>7.1.2. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ที่เกี่ยวข้อง ดำเนินการตามคำขอ และแจ้งผลการดำเนินการให้ DPO</p> <p>7.1.3 DPO แจ้งผลการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคล ตามหนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding) และบันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ว่าคำร้องขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</p> <p>7.1.4 สิ้นสุดกระบวนการ</p> <p>7.2 <b>กรณีมีค่าใช้จ่าย</b> : เนื่องจากเป็นคำร้องที่มีลักษณะเดิมซ้ำๆ โดยไม่มีเหตุอันควร หรือต้องส่งเป็นเอกสารให้แก่เจ้าของข้อมูลส่วนบุคคลในปริมาณที่มาก ทำให้เกิดค่าใช้จ่าย ให้ดำเนินการดังต่อไปนี้</p> <p>7.2.1 DPO แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบค่าใช้จ่ายในการดำเนินการตามการขอใช้สิทธิ</p> <p>7.2.2 <b>เจ้าของข้อมูลส่วนบุคคล</b> พิจารณาการยืนยันการใช้สิทธิ :</p> <p>7.2.2.1 กรณี ยืนยันให้ดำเนินการต่อ</p> <ul style="list-style-type: none"><li>● DPO รับทราบการยืนยันการขอใช้สิทธิ</li><li>● DPO แจ้งให้ผู้ที่เกี่ยวข้องดำเนินการตามคำร้องขอ</li><li>● ผู้ที่เกี่ยวข้องดำเนินการตามคำร้องขอและแจ้งผลการดำเนินการให้ DPO</li><li>● DPO แจ้งผลการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคลตามหนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding) และบันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ ว่าคำร้องขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</li></ul> <p>7.2.2.2 กรณี ไม่ให้ดำเนินการต่อ</p> <ul style="list-style-type: none"><li>● DPO รับทราบ การยกเลิกการขอใช้สิทธิ</li><li>● DPO บันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูล ส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ ว่าคำร้องขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</li></ul>



#### 5.4 เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐหรือหน้าที่ตามกฎหมาย	ก่อตั้งใช้หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1. การเพิกถอนความยินยอม	×	×	×	×	×	×	×	×	×	×	×
2. การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	×	×	×	✓	✓	×	×	×	×
3. การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	×	×	×	×	×	×	×	×	×
4. การลบข้อมูลส่วนบุคคล	✓	✓	×	✓	×	✓	×	✓	✓	✓	×
5. การระงับการประมวลผลข้อมูล	✓	✓	×	×	×	×	✓	×	✓	✓	×
6. การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	×	×	×	×	✓	×	✓	×	×
7. การคัดค้านการประมวลผลข้อมูล	✓	✓	×	×	×	×	×	×	✓	✓	✓

หมายเหตุ : ✓ หมายถึง สามารถปฏิเสธคำร้องของเจ้าของข้อมูล

× หมายถึง ไม่สามารถปฏิเสธคำร้องของเจ้าของข้อมูล



## 6. แนวทางปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ

### 6.1. วัตถุประสงค์

คู่มือปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ จัดทำขึ้นเพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคล

### 6.2. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ความรับผิดชอบ ดังนี้

1. กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสารไม่ต้องดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริง หรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูล
2. ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ให้หน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่หน่วยงานของรัฐมีอำนาจตามกฎหมายเท่านั้น หากหน่วยงานของรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการไม่ให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูลโดยไม่มีหน้าที่ตามกฎหมาย
3. ผู้ประมวลผลข้อมูล ให้หน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่หน่วยงานของรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันผู้ประมวลผลข้อมูลต้องมีข้อผูกพันกับผู้ควบคุมข้อมูลส่วนบุคคลตามสัญญาหรือข้อตกลงว่าไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่นหากหน่วยงานของรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมายและความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลส่วนบุคคล หากให้หน่วยงานของรัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวอีกด้วย



### 6.3. ขั้นตอนการปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ<sup>19</sup>

ขั้นตอน	รายละเอียด
1	ผู้ยื่นคำร้อง ยื่นแบบคำร้องขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ
2	ผู้รับเรื่องคำร้อง พิจารณาคำร้องขอหรือคำสั่งโดยระบุหน่วยงานของรัฐ หรือเจ้าหน้าที่ผู้ร้องขอโดยพิจารณาข้อมูล ดังนี้ <ul style="list-style-type: none"><li>• ชื่อ-นามสกุล เจ้าหน้าที่ และชื่อหน่วยงาน</li><li>• วันที่ได้รับคำร้องขอ</li><li>• ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย</li></ul>
3	DPO ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่ และมีข้อยกเว้นหรือไม่
4	DPO พิจารณาความถูกต้องแท้จริงของเอกสาร ดังนี้ <p>4.1 กรณี มีเอกสารมาแสดง:</p> <p>4.1.1 กรณีมีหมายศาล หรือคำสั่งศาล ให้ดำเนินการตามคำร้องขอในขั้นตอนที่ 5.1 ต่อไป 4.1.2 กรณีเอกสารอื่น ๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไป หรืออำนาจที่บัญญัติไว้กว้างๆ ว่ามีอำนาจหน้าที่อื่นใด เพื่อให้การปฏิบัติหน้าที่บรรลุนิติวัตถุประสงค์</p> <p>หากพิจารณาแล้วมีความน่าเชื่อถือ และเห็นว่ามีหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอในขั้นตอนที่ 5.1 ต่อไป</p> <p>4.2 กรณี ไม่มีเอกสาร หรือมีข้อสงสัยเกี่ยวกับเอกสาร ไม่ต้องดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่า เจ้าหน้าที่ที่มีอำนาจตามกฎหมายจริง หรือมีข้อยกเว้นตามกฎหมายประการอื่นที่ทำให้เข้าถึงหรือเปิดเผยข้อมูลได้</p>
5	DPO พิจารณาดำเนินการตามคำร้องขอ หรือไม่ <p>5.1 กรณีดำเนินการตามคำร้องขอ : แจ้งผู้ควบคุมข้อมูลส่วนบุคคลให้ดำเนินการ</p> <p>5.2 กรณีไม่ดำเนินการตามคำร้องขอ: แจ้งปฏิเสธผู้ร้องขอ พร้อมเหตุผลการปฏิเสธ</p>
6	DPO ดำเนินการเก็บบันทึกแบบคำร้องขอ และบันทึกรายละเอียดสำหรับเจ้าหน้าที่ ในแบบคำร้องขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ

<sup>19</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24, 27(6), 83, 86, 87



## 7. แนวทางปฏิบัติงานกรณีเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล

### 7.1. วัตถุประสงค์

คู่มือปฏิบัติงานกรณีเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคลจัดทำขึ้น เพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานในกรณีการเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคล และการรั่วไหลข้อมูลส่วนบุคคล เพื่อป้องกันหรือระงับเหตุการณ์การละเมิด และการรั่วไหลข้อมูล

### 7.2. ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

- 7.2.1. ผู้พบเหตุการณ์ มีหน้าที่ความรับผิดชอบ ในการแจ้ง DPO เมื่อพบเห็นเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล
- 7.2.2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ความรับผิดชอบ ดังนี้
- (1) บันทึกเหตุการณ์ และแจ้งผู้ที่เกี่ยวข้อง เพื่อดำเนินการแก้ปัญหา
  - (2) ประเมินความเสี่ยงร่วมกับบุคคลที่เกี่ยวข้อง
  - (3) ดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล
  - (4) ดำเนินการแจ้งบริษัทฯ

### 7.3. ขั้นตอนปฏิบัติงานต่อการแจ้งเหตุละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล<sup>20</sup>

ขั้นตอน	รายละเอียด
1	ผู้พบเห็นเหตุการณ์ พบเห็นเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล ให้ดำเนินการแจ้ง DPO เพื่อทราบ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป ตามแบบคำร้องการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล
2	DPO บันทึกเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล และแจ้งบุคคลที่เกี่ยวข้องเพื่อดำเนินการแก้ไขต่อไป
3	DPO ประเมินความเสี่ยงของเหตุการณ์การละเมิดข้อมูลหรือการรั่วไหลข้อมูลส่วนบุคคลร่วมกับผู้ที่เกี่ยวข้องที่ได้รับรู้ไว้ในเกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล และบันทึกในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล
4	DPO ดำเนินการตรวจสอบเกณฑ์ที่จะต้องแจ้งบริษัทฯ และ/หรือ เจ้าของข้อมูลส่วนบุคคลในเกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล และดำเนินการดังนี้ <b>4.1 กรณีแจ้งแก่บริษัทฯ :</b> DPO แจ้งเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล โดยเร็ว
5	DPO บันทึกการดำเนินการ และผลกระทบเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลที่เกิดขึ้นในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล

<sup>20</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) , 40(2) และข้อ 5 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล 2565



ขั้นตอน	รายละเอียด
6	<p>DPO ร่วมกับผู้ที่เกี่ยวข้อง ทบทวนมาตรการความปลอดภัยข้อมูลส่วนบุคคล โดยใช้ปัจจัยพิจารณาจากข้อ <u>ปัจจัยที่ต้องพิจารณาเพื่อประเมินความเสี่ยงของข้อมูลส่วนบุคคล</u> และดำเนินการดังนี้</p> <p>6.1 กรณีเกิดเหตุจากเอกสารจัดเก็บ : DPO ร่วมกับเจ้าของข้อมูลส่วนบุคคลในหน่วยงาน ทบทวน และออกมาตรการการรักษาความปลอดภัยเพิ่มเติม หากมีความจำเป็น</p> <p>6.2 กรณีเกิดเหตุทางช่องทางอิเล็กทรอนิกส์ : DPO ร่วมกับฝ่ายเทคโนโลยีสารสนเทศ ทบทวน และนำเสนอแนวทางปรับปรุงต่อฝ่ายบริหาร และปรับปรุงนโยบายความมั่นคงปลอดภัยของข้อมูลให้เป็นปัจจุบันหากมีความจำเป็นต้องเสริมมาตรการเพิ่มเติม</p>



## 8. เกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล

ระดับความรุนแรง	ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล	ผู้ที่ได้รับการแจ้ง	
		บริษัท	เจ้าของข้อมูล
5 - สูงมาก	ได้รับผลกระทบที่มีนัยสำคัญ และไม่สามารถแก้ไขหรือเยียวยาได้ อาทิ <ul style="list-style-type: none"><li>● เกิดความเสียหายทางการเงิน หรือทรัพย์สินที่ไม่สามารถชดเชยได้</li><li>● ไม่สามารถทำงาน หรือสูญเสียโอกาสทำงานตลอดชีวิต</li><li>● ทำให้สังคมเกิดความเข้าใจผิดในทางเสื่อมเสียอย่างรุนแรง</li><li>● ผลกระทบทางจิตใจหรือร่างกาย และเป็นอันตรายต่อชีวิต</li></ul>	✓	✓
4 - สูง	ได้รับผลกระทบที่มีนัยสำคัญ แต่สามารถแก้ไขหรือเยียวยาได้ อาทิ <ul style="list-style-type: none"><li>● ถูกยักยอกเงิน</li><li>● ถูกอายัดเงิน</li><li>● ถูกสถาบันการเงินปฏิเสธการทำธุรกรรม</li><li>● ถูกเลิกจ้าง</li><li>● ได้รับหมายเรียก หมายศาล</li><li>● กระทบทางจิตใจ ทำให้สุขภาพทรุดโทรม</li></ul>	✓	✓
3 - ปานกลาง	ได้รับความไม่สะดวกในการดำเนินชีวิตที่มีนัยสำคัญ แต่สามารถแก้ไขได้ อาทิ <ul style="list-style-type: none"><li>● มีภาระค่าใช้จ่ายเพิ่มเติมที่ไม่กระทบต่อการดำรงชีวิตประจำวัน</li><li>● ถูกปฏิเสธการเข้าถึงบริการทางธุรกิจหรือจากหน่วยงานภาครัฐ</li><li>● เกิดความกลัว จิตวิตก เครียด รวมถึงซึมเศร้า</li></ul>	✓	×
2 - ต่ำ	ได้รับความไม่สะดวกเพียงเล็กน้อย อาทิ <ul style="list-style-type: none"><li>● เสียเวลาในการให้ข้อมูลใหม่แก่บริษัทฯ</li><li>● มีความไม่พึงพอใจเล็กน้อย</li></ul>	✓	×
1 - ต่ำมาก	ไม่ได้รับผลกระทบ	×	×



## 9. ปัจจัยที่ต้องพิจารณา เพื่อการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

### 9.1. ความสามารถในการระบุตัวบุคคล

ให้พิจารณาว่าข้อมูลส่วนบุคคลดังกล่าว มีความสามารถในการระบุตัวบุคคลได้มากน้อยเพียงใด เช่น ชุดข้อมูลที่มี ชื่อ นามสกุล หมายเลขโทรศัพท์และที่อยู่อีเมลนั้นสามารถระบุตัวบุคคลได้โดยตรงหรือชุดข้อมูลที่อาจระบุ ตัวตนได้โดยอ้อมหรือไม่

### 9.2. ปริมาณของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลมีปริมาณมากน้อยเพียงใดที่ถูกละเมิด จำนวนปริมาณมากกับจำนวนน้อยย่อมก่อให้เกิดผลกระทบต่างกัน ไม่เพียงแต่ผลกระทบแก่เจ้าของข้อมูลส่วนบุคคล แต่รวมถึงผลกระทบต่อชื่อเสียงของบริษัทฯ

### 9.3. ความอ่อนไหวของข้อมูล

ประเมินความอ่อนไหวของข้อมูลส่วนบุคคลที่เก็บรวบรวม เช่น ข้อมูลทางการเงิน ข้อมูลเลขบัตรประจำตัวประชาชน ข้อมูลสุขภาพ ย่อมมีความอ่อนไหวมากกว่าข้อมูลหมายเลขโทรศัพท์หรือรหัสไปรษณีย์ของเจ้าของข้อมูลส่วนบุคคล ดังนั้นระดับผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดข้อมูลสำหรับข้อมูลที่มีความอ่อนไหวอยู่ในระดับที่สูงกว่าข้อมูลที่มีความอ่อนไหวน้อยกว่า

### 9.4. บริบทในการใช้ข้อมูล

พิจารณาบริบทการใช้ข้อมูลได้จากวัตถุประสงค์ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เช่น การเก็บรวบรวมข้อมูลเพื่อใช้ในการวิเคราะห์เชิงสถิติเพื่อประโยชน์ตามกฎหมาย เป็นต้น ซึ่งการประเมินบริบทของการใช้ข้อมูลจะช่วยให้หน่วยงานประเมินระดับของผลกระทบที่อาจเกิดขึ้นกับบุคคล

### 9.5. การเข้าถึงและที่เก็บข้อมูล

หากข้อมูลส่วนบุคคลถูกเข้าถึงบ่อยครั้ง หรือเข้าถึงได้ด้วยบุคคลจำนวนมาก จะเป็นการเพิ่มโอกาสที่ข้อมูลอาจรั่วไหลมากขึ้น รวมถึงหากข้อมูลสามารถเข้าถึงได้จากเครื่องมือ หรือระบบอื่น ๆ หรือส่วนงานต่างๆ เช่น การเข้าระบบผ่านทางเว็บไซต์ หรือผ่านทางแอปพลิเคชันทั้งจากภายในและภายนอกบริษัทฯ ย่อมทำให้ความเสี่ยงในการรั่วไหลมากขึ้น





## 10. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล การทำลายข้อมูลตามระยะเวลาที่กำหนด และการปฏิบัติต่อข้อมูลที่มีอยู่ก่อนพระราชบัญญัติบังคับใช้

### 10.1 มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

- 10.1.1. บริษัทมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และได้มีการจัดเก็บข้อมูลไว้เป็นระบบสารสนเทศ รวมทั้ง มีการจัดเก็บเอกสารต้นฉบับไว้ในที่ปลอดภัย มีมาตรการรักษาความปลอดภัยที่เหมาะสม และมีการทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- 10.1.2. มีการบันทึกการเปิด-คืนเอกสาร โดยให้มีการตั้งเรื่องขอจากผู้มีอำนาจอนุมัติตามนโยบายของบริษัท ก่อนใช้ข้อมูลหรือเอกสาร
- 10.1.3. มีการตรวจสอบระบบสารสนเทศ มีการสำรองข้อมูลไว้ในเครือข่าย ซึ่งมีการเก็บรักษาข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- 10.1.4. เครื่องคอมพิวเตอร์ทุกเครื่องมีการติดตั้งโปรแกรมป้องกันไวรัส เพื่อป้องกันการถูกขโมยข้อมูล และมีการตรวจสอบ และประเมินความเสี่ยงด้านความปลอดภัยข้อมูลในทุกไตรมาส
- 10.1.5. เมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ที่บริษัท แต่งตั้งไว้ จะดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะกระทบกับสิทธิเสรีภาพของบุคคลในกรณีที่มีการละเมิดมีความเสี่ยงสูง ที่จะกระทบต่อสิทธิเสรีภาพของบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องแจ้งเหตุให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาด้วย<sup>21</sup>
- 10.1.6. วิธีปฏิบัติในกรณีเกิดการละเมิดข้อมูลส่วนบุคคล<sup>22</sup>
  - กรณีที่มีการละเมิดที่มีความเสี่ยงสูงที่มีผลกระทบต่อความสิทธิและเสรีภาพ ของบุคคล เช่น ถูกขโมยข้อมูลโดย Hacker หรือข้อมูลรั่วไหลจากเอกสารหรือระบบอิเล็กทรอนิกส์ เป็นต้น บริษัทจะแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด
  - บริษัทจะต้องปกป้องดูแลข้อมูลส่วนบุคคลเป็นอย่างดี ตามมาตรฐานและมีการตรวจสอบให้มีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลอย่างถูกต้องตามกฎหมาย และกรณีเป็นข้อมูลที่ต้องขอความยินยอมก่อนบริษัทจะปฏิบัติตามขั้นตอนและแจ้งขอความยินยอมของลูกค้าด้วยทุกครั้ง เว้นแต่ได้รับการยกเว้นตามกฎหมายนี้

<sup>21</sup> แบบฟอร์มการรายงานการละเมิดข้อมูลส่วนบุคคลเพื่อส่ง สคส. เอกสารแนบ 1

<sup>22</sup> แบบฟอร์มรายงานการละเมิดข้อมูลส่วนบุคคล เพื่อแจ้งให้เจ้าของข้อมูลส่วนบุคคล เอกสารแนบ 2



หากบริษัทฝ่าฝืนไม่ปฏิบัติตามมาตรา 26 มาตรา 27 และ มาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทำให้ เจ้าของข้อมูลส่วนบุคคลเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ

- กรณีที่บริษัทหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล บริษัทหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อ เว้นแต่ เป็นเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง หรือกรณีที่เป็น การปฏิบัติตามคำสั่งของเจ้าหน้าที่ปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย
- หากผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัตินอกเหนือคำสั่ง หรือไม่ปฏิบัติตามคำสั่งอันชอบด้วยกฎหมายของบริษัท หรือผิดข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล ต้องรับผิดชอบเป็นผู้ควบคุมข้อมูลส่วนบุคคล โดยบริษัทไม่เกี่ยวข้องกับการกระทำผิดนั้น
- การจ่ายค่าสินไหมทดแทนกรณีเจ้าของข้อมูลถูกละเมิดและบริษัทเป็นผู้กระทำผิด บริษัทจะจ่ายค่าสินไหมทดแทนตามความเป็นจริง หรือตามคำสั่งที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของความเสียหายนั้น<sup>23</sup> โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับผลประโยชน์ที่บริษัทหรือผู้ประมวลผลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคล การที่บริษัทหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทา ความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการ ก่อให้เกิดความเสียหายด้วย

10.1.7. บริษัทมีการจัดทำมาตรการการบริหารความเสี่ยงเพื่อควบคุมดูแลข้อมูลส่วนบุคคลให้ปลอดภัยและเป็นไปตามมาตรฐาน ซึ่งมีการกำหนดความเสี่ยงไว้ตามรายงานบริหารความเสี่ยงที่ได้รายงานให้ที่ประชุมคณะกรรมการบริหาร และ คณะกรรมการบริษัททราบในทุกไตรมาส โดยได้มีการจัดทำความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Risk) เพิ่มใน รายงานบริหารความเสี่ยง โดยมีรายละเอียดเบื้องต้น ดังนี้

- ความเสี่ยงที่ 1 การประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล
- ความเสี่ยงที่ 2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ความเสี่ยงที่ 3 การเฝ้าระวังการปฏิบัติงาน

<sup>23</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 78



- ความเสี่ยงที่ 4 การป้องกันไม่ให้ข้อมูลรั่วไหล และการรายงานกรณีละเมิด
- ความเสี่ยงที่ 5 การส่งหรือโอนข้อมูล
- ความเสี่ยงที่ 6 การดำเนินการตามสิทธิเรียกร้องของเจ้าของข้อมูล

บริษัทจะต้องมีการประเมินความเสี่ยงว่ามีข้อมูลส่วนบุคคลที่สามารถใช้ระบุตัวตนอย่างน้อยเพียงใด มีการจัดเก็บรวบรวมที่เหมาะสมกับประเภทของข้อมูล ส่วนในเรื่องการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ต้องมีการดำเนินการขอความยินยอมทุกครั้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล มีการกำหนดผู้ใช้งาน จำกัดสิทธิในการเข้าถึงข้อมูล และควรระมัดระวังการใช้ หรือเปิดเผยข้อมูลอ่อนไหวมากเป็นพิเศษ เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ข้อมูลพันธุกรรม ข้อมูลสุขภาพ ศาสนา ความพิการ ข้อมูลชีวภาพ เป็นต้น มีมาตรการป้องกันข้อมูลรั่วไหลเป็นอย่างดี รวมทั้งต้องจัดให้มีมาตรการเยียวยา กรณีที่ข้อมูลถูกละเมิดการส่งหรือโอนข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งต้นทางและปลายทาง นอกจากนี้ เรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามให้ถูกต้องตามกฎหมาย ทั้งนี้ รายละเอียดความเสี่ยงด้านข้อมูลส่วนบุคคลมีในรายงานการบริหารความเสี่ยงของทุกไตรมาส

## 10.2. การทำลายข้อมูลตามระยะเวลาที่กำหนด

- 10.2.1. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา โดยข้อมูลส่วนบุคคลของลูกค้าที่เก็บ รวบรวมในระบบอิเล็กทรอนิกส์ และข้อมูลเอกสารสำคัญต่าง ๆ ในการทำสัญญาและอื่น ๆ ที่เกี่ยวข้อง จะถูกจัดเก็บไว้ตามอายุสัญญา เมื่อมีการปิดบัญชีครบถ้วนแล้ว อาจต้องเก็บข้อมูลทางบัญชีบางอย่างต่อไปอีก 5 ปี หรือในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้มีการชำระเงินปิดบัญชีและจัดทำสัญญาใหม่ภายในวันเดียวกัน บริษัทจะต้องเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลไว้ 10 ปี นับแต่วันที่มีการปิดบัญชีและทำสัญญาใหม่ บริษัทจะทำลายเอกสารสัญญาและข้อมูลบางส่วนที่ไม่จำเป็นต้องเก็บ รวบรวมเป็นสถิติในทางบัญชีหรือการบริหารงาน โดยมีเครื่องทำลายเอกสาร ข้อมูลส่วนบุคคล เช่น สำเนาบัตรประชาชน และข้อมูลอื่นที่ระบุตัวตน เป็นต้น
- 10.2.2. ในกรณีที่ลูกค้าผิดสัญญา มีการดำเนินคดีตามกฎหมาย และ/หรือมีการบังคับคดี บริษัทจะเก็บข้อมูลเอกสาร และฐานข้อมูลสำคัญไว้ในระบบเพื่อใช้ในการดำเนินคดี จนกว่าคดีจะถึงที่สุดและมีการชำระหนี้ครบถ้วน จึงจะทำลายเอกสารที่เป็นข้อมูลส่วนบุคคลนั้นได้
- 10.2.3. ข้อมูลทางบัญชีและเอกสารภาษี บริษัทจะเก็บไว้เป็นระยะเวลาไม่น้อยกว่า 5 ปี ทั้งนี้เป็นไปตามพระราชบัญญัติการบัญชี พ.ศ.2543
- 10.2.4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่บริษัทแต่งตั้งขึ้น มีหน้าที่ในการตรวจสอบให้แต่ละฝ่ายมีการทำลายข้อมูลเอกสารตามระยะเวลาที่กำหนดไว้ หรือตามเวลาที่เหมาะสม
- 10.2.5. การลบหรือทำลายตามคำร้องขอของเจ้าของข้อมูล รายละเอียดตามข้อ 4.7 การขอให้ลบข้อมูลส่วนบุคคลที่จะได้อธิบายต่อไปนั้น



## 11. การร้องเรียน<sup>24</sup>

### 11.1. เจ้าของข้อมูลส่วนบุคคลร้องเรียนต่อบริษัท

- 11.1.1. พนักงานผู้รับเรื่องการร้องเรียนรับเรื่องเรียนจากเจ้าของข้อมูลหรือผู้ร้องเรียน โดยมีช่องทางดังนี้
  - ทางโทรศัพท์
  - ทาง E-mail : customer\_service@nimleasing.com
  - สำนักงานสาขา
  - ทำหนังสือร้องเรียน
- 11.1.2. ผู้รับเรื่องร้องเรียนตั้งเรื่องให้ฝ่ายบริหารทราบภายใน 24 ชั่วโมง นับแต่วันทราบเหตุ
- 11.1.3. DPO/ฝ่ายที่เกี่ยวข้อง ดำเนินการตรวจสอบและสอบสวนข้อเท็จจริงและรายงานผลให้ฝ่ายบริหารทราบภายใน 48 ชั่วโมง นับแต่วันทราบเหตุ
  - ไม่มีมูล (หากข้อเท็จจริงปรากฏว่าความเสียหายที่เกิดขึ้นไม่ได้เกิดจากพนักงานให้ถือว่าเป็นอันยุติโดยตั้งเรื่องให้ฝ่ายบริหารอนุมัติเรื่องต่อไป)
  - มีมูล ตั้งเรื่องให้ฝ่ายบริหารทราบเรื่องเพื่อดำเนินการตามขั้นตอน
- 11.1.4. ผู้รับเรื่องร้องเรียนดำเนินการรายงานผลการดำเนินการให้เจ้าของข้อมูลทราบพร้อมกับหาแนวทางการเยียวยาโดยไม่ชักช้า ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- 11.1.5. ผู้รับเรื่องร้องเรียนดำเนินการแจ้งเรื่องให้ สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมง นับแต่วันทราบเหตุ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- 11.1.6. ฝ่ายกฎหมายดำเนินคดีฟ้องร้องทางแพ่งและอาญาตามนโยบายบริษัท (หากการละเมิดและความเสียหายนั้นเกิดจากพนักงานบริษัท)  
ทั้งนี้คณะกรรมการที่กำกับดูแลรับผิดชอบในเรื่องการเยียวยานั้นให้เป็นไปตามนโยบายบริษัท

### 11.2. เจ้าของข้อมูลร้องเรียนต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล

- 11.2.1. สำนักงานคุ้มครองข้อมูลส่วนบุคคลแจ้งเรื่องมาที่บริษัทให้ทำการแก้ไขข้อผิดพลาดหรือทำการไกล่เกลี่ยข้อพิพาท
- 11.2.2. ผู้รับเรื่องร้องเรียนตั้งเรื่องให้ฝ่ายบริหารทราบ ภายใน 24 ชั่วโมง นับแต่วันทราบเหตุ
- 11.2.3. DPO/ฝ่ายที่เกี่ยวข้อง ดำเนินการตรวจสอบและสอบสวนข้อเท็จจริงและรายงานผลให้ฝ่ายบริหารทราบภายใน 48 ชั่วโมง นับแต่วันทราบเหตุ
- 11.2.4. DPO/ฝ่ายที่เกี่ยวข้อง ไปดำเนินการเจรจาไกล่เกลี่ยที่สำนักงานคุ้มครองข้อมูลส่วนบุคคลตามวันนัดหมาย หรือฝ่ายที่เกี่ยวข้องดำเนินการแก้ไขข้อผิดพลาด
- 11.2.5. DPO/ฝ่ายที่เกี่ยวข้อง แจ้งรายงานผลการไกล่เกลี่ย หรือแก้ไขข้อผิดพลาดให้ฝ่ายบริหารทราบ และหากเจรจาไกล่เกลี่ยกันได้ ให้ฝ่ายบริหารอนุมัติเรื่องไป หากไม่สามารถเจรจา

<sup>24</sup> ผังขั้นตอนการร้องเรียนตามเอกสารแนบ 5



ไกลเกลี่ยได้ ให้ฝ่ายบริหารพิจารณาสั่งการแนวทางในการดำเนินการต่อไป จนกว่าเรื่องจะเสร็จยุติลงตามนโยบายบริษัท

- 11.2.6. ฝ่ายกฎหมายดำเนินคดีฟ้องร้องทางแพ่งและอาญา ตามนโยบายบริษัท (หากการละเมิดและความเสียหายนั้นเกิดจากพนักงานบริษัท)

## 12. สรุปการกำหนดโทษตามกฎหมายนี้

### 12.1. โทษทางแพ่ง<sup>25</sup>

#### 12.1.1. ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล

ดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตามเว้นแต่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

- ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง
- เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ค่าสินไหมทดแทนนั้นหมายความรวมถึง ค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลฯ ได้ใช้จ่ายไปตาม ความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทน เพื่อการลงโทษจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่เห็นสมควร แต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับสถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ เป็นอันขาดอายุ ความเมื่อพ้น 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดชอบ หรือเมื่อพ้น 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

<sup>25</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 และ 78



## 12.2. โทษทางอาญา

### 12.2.1. ผู้ควบคุมข้อมูลส่วนบุคคล

ในการใช้หรือเปิดเผย หรือส่งโอนข้อมูลตามมาตรา 26 (ข้อมูลอ่อนไหว) โดยได้ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>26</sup>

- ใช้หรือเปิดเผยข้อมูลฯ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ (เว้นแต่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26) หรือ
- กรณีที่บุคคลหรือนิติบุคคลที่ได้รับข้อมูลฯ มาจากผู้ควบคุมข้อมูลส่วนบุคคลได้เปิดเผยฯ ให้ และบุคคลหรือนิติบุคคลนั้นได้ใช้ข้อมูลฯ นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ กับผู้ควบคุมข้อมูลฯ หรือ
- ไม่ปฏิบัติตามหลักเกณฑ์การส่งหรือโอนข้อมูลไปยังต่างประเทศตามที่คณะกรรมการประกาศกำหนด ประเทศปลายทางหรือองค์การระหว่างประเทศมีมาตรฐาน การคุ้มครองที่ไม่เพียงพอ เว้นแต่เป็นการปฏิบัติตามกฎหมาย หรือได้รับความยินยอมจาก เจ้าของข้อมูลที่ได้ทราบถึงมาตรฐานการคุ้มครองข้อมูลฯ ที่ไม่เพียงพอของประเทศปลายทางนั้นแล้ว

ทั้งนี้ การดำเนินการดังกล่าวข้างต้นทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย **มีโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสน บาท หรือทั้งจำทั้งปรับ** (ความในมาตรานี้เป็นความผิดอันยอมความได้)

### 12.2.2. ผู้ควบคุมข้อมูลส่วนบุคคล

เพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่นโดยใช้ข้อมูลส่วนบุคคลตามมาตรา 26 (ข้อมูลอ่อนไหว) โดยได้ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>27</sup>

- ในการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (เว้นแต่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26) หรือ
- ไม่ปฏิบัติตามหลักเกณฑ์การส่งหรือโอนข้อมูลไปยังต่างประเทศตามที่คณะกรรมการประกาศกำหนด ประเทศปลายทางหรือองค์การระหว่างประเทศมีมาตรฐาน คุ้มครองที่ไม่เพียงพอ เว้นแต่เป็นการปฏิบัติตามกฎหมาย หรือได้รับความยินยอมจากเจ้าของ ข้อมูลที่ได้ทราบถึงมาตรฐานการคุ้มครองข้อมูลฯ ที่ไม่เพียงพอของประเทศปลายทางนั้นแล้ว

ทั้งนี้ การดำเนินการดังกล่าวข้างต้นทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอาย **มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาทหรือทั้งจำทั้งปรับ** (ความในมาตรานี้เป็นความผิดอันยอมความได้)

<sup>26</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 79 วรรค 1

<sup>27</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 79 วรรค 2



### 12.2.3. ผู้ใด (บุคคลทั่วไป)

เปิดเผยข้อมูลส่วนบุคคลที่ได้ล่วงรู้จากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษ จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ เว้นแต่<sup>28</sup>

- การเปิดเผยตามหน้าที่
- การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการการพิจารณาคดี
- การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจตามกฎหมาย
- การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

### 12.2.4. นิติบุคคล/บุคคลใด

ในกรณีผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการ สั่งการ หรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใด ซึ่งรับผิดชอบในการ ดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และละเว้นไม่สั่งการ หรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

**หมายเหตุ** กรรมการบริษัท ผู้บริหาร ผู้บังคับบัญชา ผู้จัดการ หรือผู้รับมอบอำนาจ ที่ได้สั่งการหรือละเว้นไม่กระทำการ ไม่สั่งการจนเป็นเหตุให้เกิดความเสียหาย ต้องรับโทษตามความผิดของนิติบุคคลนั้นด้วย

## 12.3. โทษทางปกครอง

### 12.3.1. ผู้ควบคุมข้อมูลส่วนบุคคล

ไม่ปฏิบัติตาม<sup>29</sup>

- การเก็บรวบรวมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะเก็บรวบรวม
- บริษัทไม่ดำเนินการตามคำขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล ภายใน 30 วัน นับแต่วันได้รับคำขอ
- บันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงาน สคส. ตรวจสอบได้
- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

<sup>28</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 80 วรรค 1 และ วรรค 2

<sup>29</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 82



- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จัดหาอุปกรณ์ เครื่องมือให้เพียงพอ อำนวยความสะดวก และจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาจ้างด้วยเหตุที่ได้ปฏิบัติตามหน้าที่ไม่ได้ ทั้งนี้ ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้โดยตรง
- ไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ตามมาตรา 19 (แบบและข้อความการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล)
- ไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรค 6 ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนถอนความยินยอม
- ไม่ปฏิบัติตามหลักในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ต้องแจ้งให้เจ้าของข้อมูลทราบ ก่อนหรือขณะดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคล โดยอย่างช้าไม่เกิน 30 วัน เว้นแต่เป็นการเก็บรวบรวมที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือ มาตรา 26

ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

### 12.3.2. ผู้ควบคุมข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>30</sup>

- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งกับเจ้าของข้อมูลไว้ก่อนหรือขณะเก็บรวบรวม
- เก็บรวบรวมข้อมูลนอกเหนือวัตถุประสงค์อันชอบด้วยกฎหมาย
- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น โดยไม่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
- บุคคลหรือนิติบุคคล ใช้ หรือเปิดเผยข้อมูล นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับ ผู้ควบคุมข้อมูลส่วนบุคคล
- ส่งหรือโอนข้อมูลไปยังประเทศปลายทางหรือองค์กรระหว่างประเทศที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอ หรือไม่ปฏิบัติตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด
- ไม่ปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่กำหนดไว้ตามมาตรา 37

<sup>30</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 83





- ขอความยินยอมโดยการลอกกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิด ในวัตถุประสงค์
- ส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม (มีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลไปยังต่างประเทศตามที่คณะกรรมการประกาศกำหนด)  
ต้องระวางโทษทางปกครองไม่เกิน 3 ล้านบาท

### 12.3.3. ผู้ควบคุมข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>31</sup>

- เก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา 26 (ข้อมูลอ่อนไหว) โดยไม่ได้รับความยินยอมและไม่เข้าตามข้อยกเว้นไม่ต้องขอความยินยอม
- ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมและไม่ได้รับการยกเว้นตามมาตรา 24 หรือมาตรา 26
- ส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 (ข้อมูลอ่อนไหว) ไปยังต่างประเทศ ประเทศ ปลายทาง หรือองค์การระหว่างประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ไม่เพียงพอ โดยไม่ได้รับความยินยอมหรือไม่ได้เป็นการปฏิบัติตามกฎหมาย
- ส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 (ข้อมูลอ่อนไหว) โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม (มีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือ โอนข้อมูลไปยังต่างประเทศตามที่คณะกรรมการประกาศกำหนด)

ต้องระวางโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

### 12.3.4. ผู้ประมวลผลข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>32</sup>

- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ให้การสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จัดหาอุปกรณ์ เครื่องมือให้เพียงพอ อำนวยความสะดวก และจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ออกจากงานหรือเลิกสัญญาจ้างด้วยเหตุที่ได้ปฏิบัติตามหน้าที่ไม่ได้ ทั้งนี้ ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมส่วนบุคคล หรือผู้ประมวลผลส่วนบุคคลได้โดยตรง

ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

<sup>31</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 84

<sup>32</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 85



### 12.3.5. ผู้ประมวลผลข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>33</sup>

- หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลทั้งหมด ตามมาตรา 40 (ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลฯ ตามคำสั่งของผู้ควบคุมส่วนบุคคลเท่านั้น และจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคล และจัดทำและเก็บรักษาบันทึกการรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด)
- ส่งหรือโอนข้อมูลส่วนบุคคล โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม (มีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลไปยัง ต่างประเทศตามที่คณะกรรมการประกาศกำหนด)
- กรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักรต้องแต่งตั้งตัวแทนเป็นหนังสือซึ่ง ตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ ประมวลผลข้อมูลส่วนบุคคล โดยไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ประมวลผลข้อมูลส่วนบุคคล (มาตรา 37 (5) ได้นำมาใช้บังคับโดยอนุโลมตาม มาตรา 38 วรรคสอง)

ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

### 12.3.6. ผู้ประมวลผลข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>34</sup>

- ส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 วรรคหนึ่งหรือวรรคสาม โดยไม่เป็นไปตาม มาตรา 29 วรรคหนึ่งหรือวรรคสาม (มีหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลไปยังต่างประเทศตามที่คณะกรรมการประกาศกำหนด)

ต้องระวางโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

### 12.3.7. ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล / ตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคล

#### ฝ่าฝืนหรือไม่ปฏิบัติตาม<sup>35</sup>

- บันทึกการรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงาน สคส. สามารถตรวจสอบได้
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

<sup>33</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 86

<sup>34</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 87

<sup>35</sup> พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 88



### 12.3.8. ผู้ใด (ทุกคน/ทุกหน่วยงาน)

- ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่ชี้แจงข้อเท็จจริงหรือส่งเอกสารข้อมูลเกี่ยวกับเรื่องที่มีผู้มาร้องเรียน หรือเรื่องอื่นใดตามพระราชบัญญัตินี้ หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา 76 วรรค 4  
ต้องระวางโทษปรับทางปกครองไม่เกิน 5 แสนบาท

## 13. บทลงโทษ

พนักงานสาขา หรือพนักงานฝ่ายอื่นใดที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ใดหรือฝ่ายใดฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ บริษัทจะพิจารณาลงโทษทางวินัยตามระเบียบบริษัท รวมทั้งอาจมีความรับผิดชอบทั้งทางแพ่งและทางอาญา ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง

## 14. การตรวจสอบ ติดตามเพื่อให้พนักงานปฏิบัติตามกฎเกณฑ์ PDPA

- 14.1. DPO ทำการสุ่มตรวจไปยังสาขาโดยการโทรศัพท์เพื่อตรวจสอบและประเมินว่ามีการปฏิบัติตามนโยบายของบริษัท
- 14.2. รายงานผลการตรวจสอบไปยังฝ่ายบริหารเพื่อทราบและสั่งการเมื่อต้องทำการแก้ไขปรับปรุงทำงานของสาขา

## 15. การให้ความรู้แก่พนักงานและการปรับปรุงนโยบายบริษัทให้เป็นไปตาม PDPA

- 15.1. ให้ฝ่ายกฎหมายทำการจัดอบรมให้ความรู้เกี่ยวกับแนวทางการปฏิบัติงาน เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง
- 15.2. ให้ฝ่ายกฎหมายทำการทบทวนและปรับปรุงนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้ทันสมัยปีละ 1 ครั้ง



## 16. การทบทวนแนวปฏิบัติ

คณะกรรมการ เจ้าหน้าที่ คณะทำงาน PDPA ต้องดำเนินการทบทวนแนวปฏิบัติให้เป็นไปตามนโยบาย และการแก้ไขเพิ่มเติมของกฎหมาย โดยจะติดตามประกาศเพิ่มเติมของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้องมาปรับให้สอดคล้องกับนโยบาย และต้องเสนอต่อฝ่ายบริหารต่อไป

## 17. การติดต่อสอบถามหรือใช้สิทธิ

Call Center โทรศัพท์ 097-3458888

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

E-mail : [customer\\_service@nimleasing.com](mailto:customer_service@nimleasing.com)

สถานที่ติดต่อ : บริษัท นีมลีสซิ่ง จำกัด เลขที่ 72/1 ถนนเมืองสมุทร ตำบลช้างม่อย อำเภอเมืองเชียงใหม่ จังหวัดเชียงใหม่ 50300 (วันจันทร์ - เสาร์ เวลา 08.00 – 17.00 น.)