



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

คู่มือการให้คำปรึกษาการปฏิบัติตาม
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ฉบับวันที่ 30 พฤษภาคม 2565

สารบัญ

1. แหล่งข้อมูลเพิ่มเติมของกฎหมายคุ้มครองข้อมูลส่วนบุคคล.....	3
2. คำถามที่พบบ่อย	3
3. 10 เรื่องที่ประชาชนต้องรู้เกี่ยวกับ PDPA.....	5
4. ภาคผนวก.....	6
1) นิยามตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล.....	6
2) การแจ้งรายละเอียดและวัตถุประสงค์.....	11
3) หลักการขอความยินยอม.....	13
4) ฐานการประมวลผลที่ไม่ต้องขอความยินยอม.....	17
5) สิทธิของเจ้าของข้อมูลส่วนบุคคล.....	21
6) เหตุการณ์ละเมิดข้อมูลส่วนบุคคล.....	27
7) การเตรียมความพร้อมหรือแนวปฏิบัติ.....	31
8) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล.....	34
9) Cookie กับข้อมูลส่วนบุคคล.....	35
10) แนวทางการป้องกันหรือมาตรการความปลอดภัย.....	37
11) PDPA กับกรณีนอกราชอาณาจักร.....	38
12) เกร็ดความรู้อื่นๆ.....	40

1. แหล่งข้อมูลเพิ่มเติมของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- สามารถติดตามข้อมูลเผยแพร่ของ สคส. ได้ที่ www.pdpc.or.th
- facebook - " PDPC Thailand " <https://www.facebook.com/pdpc.th>
- ดาวน์โหลดได้ที่ <https://bit.ly/infopdpc>

2. คำถามที่พบบ่อย

Q1 – PDPA คืออะไร

A1 – Personal Data Protection Act หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Q2 - กฎหมายจะเลื่อนบังคับใช้หรือไม่

A2 - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะบังคับใช้ครบทุกมาตรา ในวันที่ 1 มิถุนายนนี้

Q3 – กฎหมายใหม่จะหาข้อมูลได้จากไหน

A3 - สามารถติดตามข้อมูลเผยแพร่ของ สคส. ได้ที่ www.pdpc.or.th หรือ facebook page " PDPC Thailand ”

Q4 - กฎหมายลำดับรอง เช่น ประกาศต่าง ๆ มีแล้วหรือยัง

A4 – ขณะนี้อยู่ในขั้นตอนการรับฟังความเห็น สามารถติดตามได้จากเว็บไซต์ www.pdpc.or.th

Q5 – การเผยแพร่ภาพผู้อื่นผิดหรือไม่

A5 – การเผยแพร่ภาพผู้อื่นไม่ควร 1) นำไปแสวงหาผลประโยชน์ หรือ 2) ทำให้ผู้อื่นเสียหาย

Q6 – การถ่ายภาพบุคคลมีข้อยกเว้นอย่างไร

A6 – กฎหมายคุ้มครองข้อมูลส่วนบุคคลยกเว้นการถ่ายภาพบุคคลให้ทำได้ในกรณีดังต่อไปนี้

1) การถ่ายภาพบุคคลเพื่อวัตถุประสงค์ “ใช้เพื่อประโยชน์ส่วนตัว หรือเพื่อกิจกรรมในครอบครัว”

ตัวอย่าง การถ่ายภาพที่เข้าข้อยกเว้นตามกฎหมาย เช่น การถ่ายภาพบุคคล ครอบครัว เพื่อนฝูง คนรู้จัก ในส่วนกิจกรรมในครอบครัว งานอดิเรก การพักผ่อนหย่อนใจ เพื่อความบันเทิงในครอบครัว (วันเกิด, วันครบรอบแต่งงาน ฯลฯ) การถ่ายรูปลงสื่อ Social Media (เช่น Facebook, Instagram, TikTok) เพื่อใช้ในครอบครัว สันทนาการ ในวงจำกัด เท่านั้น

2) การถ่ายภาพของกิจการ “สื่อสารมวลชน” เพื่อประโยชน์สาธารณะและต้องอยู่ภายใต้ประมวลจริยธรรม คำอธิบาย สื่อมวลชน หมายถึง สื่อที่มีการจดทะเบียนตามกฎหมาย มีกองบรรณาธิการ เซ็นเซอร์ และมีประมวลจริยธรรมกำกับ

ตัวอย่าง นักข่าวถ่ายภาพบุคคลเพื่อใช้รายงานข่าวเพื่อประโยชน์สาธารณะ หรือเพื่อดำเนินการในฐานะ สื่อสารมวลชนภายใต้ประมวลจริยธรรม

- 3) การถ่ายภาพเพื่อสร้างสรรค์งานวรรณกรรม งานทรัพย์สินทางปัญญา ลิขสิทธิ์ เช่น งานวรรณกรรม งานศิลปกรรม ภายใต้กรอบกฎหมายที่กำหนด
ตัวอย่าง การถ่ายภาพของช่างถ่ายภาพในที่สาธารณะเพื่อสร้างสรรค์งานศิลปะ วรรณกรรม โดยไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล
- 4) การถ่ายภาพเพื่อวัตถุประสงค์ในการใช้เป็นพยานหลักฐานในการดำเนินการทางกฎหมายกับผู้กระทำความผิดเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมาย หรือโดยมีกฎหมายรองรับ
ตัวอย่าง การถ่ายภาพบุคคลที่เกิดเหตุเพื่อเป็นข้อมูลประกอบการกระทำความผิด หรือเพื่อวัตถุประสงค์ในการพิจารณาคดีของกระบวนการยุติธรรม
- 5) การถ่ายภาพโดยเข้าข่ายยกเว้นที่กฎหมายกำหนด เช่น การบันทึกภาพตามข้อตกลง สัญญา บันทึกภาพเพื่อประโยชน์สาธารณะ เพื่อปฏิบัติหน้าที่ตามกฎหมาย เพื่อปกป้องชีวิตร่างกาย ฯลฯ
- 6) การถ่ายภาพโดยเจ้าของข้อมูลส่วนบุคคล (ผู้ถูกถ่ายภาพ) ให้ความยินยอมให้บันทึกภาพโดยชัดแจ้ง โดยการขอความยินยอมต้องทำเป็นหนังสือหรือผ่านสื่ออิเล็กทรอนิกส์ เช่น การบันทึกเสียง ภาพ ส่งข้อความ ให้ความยินยอมผ่านทางไลน์ หรือ สื่อสังคมโซเชียลมีเดีย ฯลฯ

Q7 – บริษัทยังไม่ได้เริ่มทำอะไรเลย ต้องทำอะไรบ้าง

A7 – 1) ศึกษากฎหมายเบื้องต้นจาก www.pdpc.or.th

2) หากบริษัทมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า ผู้มาติดต่อหรือพนักงาน บริษัทต้องจัดทำประกาศการแจ้งรายละเอียดและวัตถุประสงค์ตามมาตรา 23 และจัดทำบันทึกการตามมาตรา 39

3) จัดทำแบบขอความยินยอมตามมาตรา 19 หากบริษัทมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่เข้าข่ายยกเว้นของกฎหมายตามมาตรา 24 หรือ 26

4) จัดทำข้อตกลงการประมวลผลตามมาตรา 40 หากบริษัทมีการส่งหรือว่าจ้างบริษัทอื่นเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้

Q8 – การเก็บรวบรวมข้อมูลส่วนบุคคลต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลทุกกรณีหรือไม่

A8 – ไม่จำเป็นต้องขอความยินยอม หากการใช้ข้อมูลดังกล่าว

- (1) เป็นการทำตามสัญญาให้บริการ
- (2) เป็นการตามกฎหมายอื่นที่ให้อำนาจไว้
- (3) เป็นการใช้เพื่อรักษาชีวิตและ/หรือ ร่างกายของบุคคล
- (4) เป็นการใช้เพื่อการค้นคว้าวิจัยทางสถิติ
- (5) เป็นการใช้เพื่อประโยชน์สาธารณะ
- (6) เป็นการใช้เพื่อปกป้องผลประโยชน์ของตนเอง แต่ต้องไม่ละเมิดสิทธิขั้นพื้นฐานของผู้อื่น

3. 10 เรื่องที่ประชาชนต้องรู้เกี่ยวกับ PDPA

10

เรื่องที่ประชาชน
ต้องรู้เกี่ยวกับ
PDPA

01 ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมเฉพาะ เช่น ชื่อ ที่อยู่ หมายเลขประจำตัว ข้อมูลสุขภาพ ฯลฯ (มาตรา 6)

02 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล **ตามวัตถุประสงค์ที่ได้แจ้งเราไว้ก่อนหรือในขณะที่เก็บรวบรวม** (ห้ามใช้บอกเหนือวัตถุประสงค์) (มาตรา 21)

03 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องเก็บรวบรวมข้อมูลส่วนบุคคลของเราเท่าที่จำเป็นภายใต้วัตถุประสงค์อื่นชอบด้วยกฎหมาย (มาตรา 22) (ใช้ข้อมูลของอาชญากรน้อยที่สุด)

04 ความยินยอม เป็นฐานการประมวลผลฐานหนึ่งเท่านั้น ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการกำหนดฐานการประมวลผล ให้สอดคล้องกับลักษณะการประมวลผลและความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับเจ้าของข้อมูลส่วนบุคคล (ตามมาตรา 24 หรือมาตรา 26)

05 ในการขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้อง**คำนึงอย่างที่สุด**ในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล (ต้องไม่มีสภาพบังคับในการให้ / ไม่ให้) (มาตรา 19 วรรคสี่)

06 เจ้าของข้อมูลส่วนบุคคล มีสิทธิ...

- 1) สิทธิในการถอนความยินยอม ในกรณีที่ได้ให้ความยินยอมไว้ (มาตรา 19 วรรคห้า)
- 2) สิทธิได้รับการแจ้งให้ทราบรายละเอียด (Privacy Notice) (มาตรา 23)
- 3) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (มาตรา 30)
- 4) สิทธิขอให้โอนข้อมูลส่วนบุคคล (มาตรา 31)
- 5) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 32)
- 6) สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (มาตรา 33)
- 7) สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (มาตรา 34)
- 8) สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล (มาตรา 35)

07 PDPA ใช้กับการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่อยู่ในประเทศไทย ไม่ว่าจะ มีสัญชาติใดก็ตาม (มาตรา 5)

08 ในกรณีที่เหตุการณ์ละเมิด ข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อนิติและสุขภาพของเจ้าของข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า (มาตรา 37 (4))

10 เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนต่อคณะกรรมการผู้ชี้ขาดทนาย ในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตาม PDPA หรือประกาศฯ ที่ออกตาม PDPA (ทั้งนี้ กระบวนการร้องเรียนเป็นไปตามระเบียบที่คณะกรรมการฯ ประกาศกำหนด) (มาตรา 73)

09 ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่จัดทำบันทึกการกิจกรรม เพื่อให้สำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ (Personal Data Protection Act : PDPA)
 ช่องทางการติดต่อ : PDPC Thailand

สำนักงานคณะกรรมการ
ผู้ตรวจการแผ่นดิน

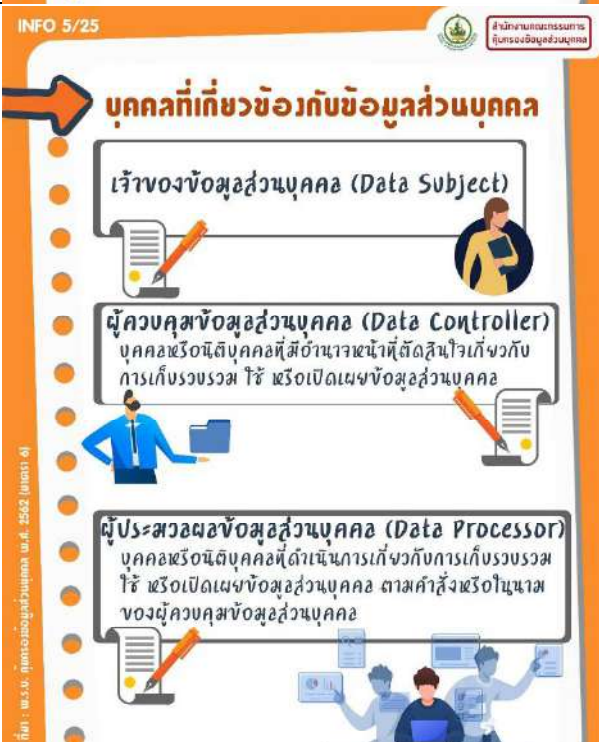
4. ภาคผนวก

1) นิยามตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
1.1	ความหมาย “ข้อมูลส่วนบุคคล”	ความหมายของ ข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6 ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามแนวทางของ GDPR ยกตัวอย่างว่า กรณีดังต่อไปนี้เป็นข้อมูลส่วนบุคคล < GDPR Article 4 (1) > 1. ชื่อ 2. หมายเลขประจำตัว 3. ข้อมูลสถานที่ 4. สิ่งระบุตัวลักษณะออนไลน์ 5. พิกัดอย่างหนึ่งหรือหลายอย่างรวมกันที่ระบุตัวลักษณะทางกายภาพ สรีรวิทยา พันธุกรรม ชีตใจ เศรษฐกิจ วัฒนธรรม หรือสถานะทางสังคมของบุคคลธรรมดา ข้อมูลใดเป็นข้อมูลส่วนบุคคลหรือไม่ จำต้องพิจารณาจากบริบทของการใช้ข้อมูลนั้น ๆ ประกอบด้วยว่าสามารถทำให้ระบุตัวบุคคลนั้น ๆ ได้หรือไม่ ซึ่งกฎหมายไทยบัญญัติสอดคล้องกับกฎหมายในหลาย ๆ ประเทศที่กำหนดค่านิยามของข้อมูลส่วนบุคคลไว้แบบ “ปลายเปิด” เพื่อให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว ที่มา : มาตรา 6 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ Article 4 General Data Protection Regulation (GDPR)
1.2	ผู้ควบคุมข้อมูลส่วนบุคคล คือใคร	ผู้ควบคุมข้อมูลส่วนบุคคล คือใคร? ผู้ควบคุมข้อมูลส่วนบุคคล --- DC Data Controller ผู้ประมวลผลข้อมูลส่วนบุคคล --- DP Data Processor DC อาจจะเป็นบุคคลธรรมดา หรือนิติบุคคลก็ได้ DC มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล DP ประมวลผลข้อมูลส่วนบุคคล* ตามคำสั่งหรือในนามของ >> DC DP ต้องไม่ใช้ DC ในกิจกรรมการประมวลผลข้อมูล ทุกองค์กรที่มีการประมวลผลข้อมูลส่วนบุคคลจึงอาจมีสถานะเป็น DC หรือ DP หากไม่ใช่องค์กรหรือกิจกรรมการประมวลผล ที่ได้รับยกเว้นการใช้บังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ องค์กรดังกล่าวในบริบทของการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรมนั้น ๆ ต้องมีสถานะเป็น DC หรือ DP แล้วแต่กรณี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดหน้าที่และความรับผิดชอบตามกฎหมายหลัก ๆ ไว้ที่ “DC” โดยได้เว้นวรรคจาก GDPR** พิจารณาว่า “DC” คือ องค์กรที่กำหนดวัตถุประสงค์ และวิธีการในการประมวลผล และให้พิจารณาจากความเป็นจริง ไม่ใช่ตามทฤษฎีที่กำหนดหรือตกลงกันเอง ** GDPR General Data Protection Regulation เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป การประมวลผลข้อมูลส่วนบุคคล ครอบคลุมถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่มา : Guidelines 37:2020 on the meaning of controller and processor in the GDPR

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
1.3	ใครเป็นใครใน PDPA	ใครเป็นใครใน PDPA 1. เจ้าของข้อมูลส่วนบุคคล (Data Subject) ประชาชนทุกคน หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsorce ด้วย กล่าวอีกนัยคือเป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมถึงคนตายและนิติบุคคล *ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น 2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หน่วยงาน / องค์กร / สถาบัน ที่กำหนดวัตถุประสงค์ วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล บุคคลธรรมดาที่อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน 3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล โดยหลักคือ Outsorce ที่รับจ้าง *ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน / องค์กร / สถาบัน 4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ หน่วยงาน / องค์กร / สถาบัน ให้เป็นไปตามกฎหมาย
1.4	อะไรบ้างที่เป็นข้อมูลชีวภาพ	อะไรบ้าง ที่เป็น..ข้อมูลชีวภาพ ตัวอย่าง ของข้อมูลชีวภาพที่เป็นข้อมูลส่วนบุคคลก็เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่น ทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นได้เหมือนกับบุคคลอื่นได้ ทางกายภาพ - ข้อมูลภาพจำลองใบหน้า - ข้อมูลจำลองม่านตา - ข้อมูลจำลองลายนิ้วมือ - การจดจำเสียง ทางพฤติกรรม - การวิเคราะห์ลายมือชื่อ (Caroline) - การวิเคราะห์การเดิน - การวิเคราะห์การกดแป้นพิมพ์อุปกรณ์คอมพิวเตอร์ ที่มา : https://ico.org.uk

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
1.5	ข้อมูลชีวภาพ	 ข้อมูลชีวภาพ - Biometrics Data - “ข้อมูลชีวภาพ” (ตามมาตรา 26 ของร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) 1. เป็นข้อมูลส่วนบุคคลประเภทหนึ่ง ที่กฎหมายมุ่งคุ้มครองเป็นพิเศษ 2. เกิดจากการใช้เทคโนโลยีหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะ-เด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ (เป็นอัตลักษณ์ของบุคคล) เช่น ข้อมูลภาพจำลองลายนิ้วมือ ข้อมูลภาพจำลองใบหน้า การวิเคราะห์การเดิน เป็นต้น 3. ทำให้สามารถยืนยันตัวตนของบุคคลนั้น ที่ไม่เหมือนกับบุคคลอื่นได้ ข้อมูลชนิดนี้มีความสำคัญในสภาพแวดล้อมเทคโนโลยีดิจิทัลเป็นอย่างมาก เนื่องจากผู้ให้บริการหลายประเภทนำข้อมูลนี้มาใช้เพื่อกำหนดให้เป็นเงื่อนไขการเข้าใช้บริการ รวมถึงการยืนยันหรือระบุตัวบุคคลด้วย
1.6	ข้อมูลส่วนบุคคล	 INFO 4/25 ข้อมูลส่วนบุคคล (Personal Data) ข้อมูลเกี่ยวกับบุคคลที่ผู้ใช้ระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น เลขประจำตัวประชาชน ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ e-mail ข้อมูลทางการเงิน เชื้อชาติ ศาสนาเรื่อปริญญา ♀♂ พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลคนต่าง ข้อมูลนิติบุคคล ไม่เป็นข้อมูลส่วนบุคคลตามกฎหมายนี้

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
1.7	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน	 INFO 9/25 ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ข้อมูลส่วนบุคคลเกี่ยวกับ - เชื้อชาติ เผ่าพันธุ์ - ความเชื่อในลัทธิ ศาสนาหรือปรัชญา - ประวัติสุขภาพกรรม - ข้อมูลสุขภาพแรงงาน - ความคิดเห็นทางการเมือง - พฤติกรรมทางเพศ - ข้อมูลสุขภาพ ความพิการ - ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 26)
1.8	บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	 INFO 5/25 บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล (Data Subject) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 6)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
1.9	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	
1.10	หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล	

2) การแจ้งรายละเอียดและวัตถุประสงค์

ลำดับ	ชื่อเรื่อง	ภาพประกอบ												
2.1	การประกาศ ความเป็นส่วนตัว Privacy Notice	การประกาศความเป็นส่วนตัว Privacy Notice บ. 23 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว - วัตถุประสงค์ของการเก็บรวบรวม และวัตถุประสงค์ ตาม บ. 24 ที่ให้อำนาจในการเก็บรวบรวมได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล - แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา และแจ้งถึงผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล - ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลา ในการเก็บรวบรวมไว้ ในกรณีที่ไม่สามารถกำหนด ระยะเวลาได้ ให้กำหนดระยะเวลาที่อาจคาดหมาย ได้ตามมาตรฐานของการเก็บรวบรวม - ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูล ส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย - ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนหรือเจ้าหน้าที่ ผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ - สิทธิของเจ้าของข้อมูลส่วนบุคคล ได้แก่ สิทธิเข้าถึงและขอรับ สำเนา สิทธิขอโอนข้อมูล สิทธิคัดค้าน สิทธิขอให้ลบหรือทำลาย สิทธิขอระงับการใช้ข้อมูล สิทธิขอให้ดำเนินการแก้ไขข้อมูลให้ ถูกต้อง และสิทธิในการร้องเรียน หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตาม ต้องระวางโทษปรับทางปกครองไม่เกิน 1 ล้านบาท (บ. 82)												
2.2	Privacy Policy กับ Privacy Notice ต่างกันอย่างไร	Privacy Policy กับ Privacy Notice ต่างกันอย่างไร? PRIVACY POLICY นโยบายการคุ้มครองข้อมูลส่วนบุคคล PRIVACY NOTICE ประกาศความเป็นส่วนตัว <table border="1"> <thead> <tr> <th>ข้อแตกต่าง</th> <th>PRIVACY POLICY</th> <th>PRIVACY NOTICE</th> </tr> </thead> <tbody> <tr> <td>สภาพบังคับทางกฎหมาย</td> <td>กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)</td> <td>กฎหมายกำหนดให้ผู้ควบคุมข้อมูล มีหน้าที่ต้องแจ้ง ตามมาตรา 23</td> </tr> <tr> <td>ขอบเขต</td> <td>เป็นเอกสารที่สื่อสารถึงบุคคล ภายในองค์กร</td> <td>เป็นประกาศที่มีผลเฉพาะ เจ้าของข้อมูลส่วนบุคคลเท่านั้น</td> </tr> <tr> <td>เนื้อหา</td> <td>เป็นนโยบายและแนวปฏิบัติขององค์กร ในการคุ้มครองข้อมูลส่วนบุคคล</td> <td>เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบเงื่อนไขเกี่ยวกับการประมวลผล ข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด</td> </tr> </tbody> </table> หมายเหตุ : Privacy policy อาจจะครอบคลุม Privacy notice ได้ โดยพิจารณาเนื้อหาภายใน หากครบถ้วนตามที่กฎหมายกำหนด ก็ถือว่าเป็นการแจ้งวัตถุประสงค์ ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว	ข้อแตกต่าง	PRIVACY POLICY	PRIVACY NOTICE	สภาพบังคับทางกฎหมาย	กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)	กฎหมายกำหนดให้ผู้ควบคุมข้อมูล มีหน้าที่ต้องแจ้ง ตามมาตรา 23	ขอบเขต	เป็นเอกสารที่สื่อสารถึงบุคคล ภายในองค์กร	เป็นประกาศที่มีผลเฉพาะ เจ้าของข้อมูลส่วนบุคคลเท่านั้น	เนื้อหา	เป็นนโยบายและแนวปฏิบัติขององค์กร ในการคุ้มครองข้อมูลส่วนบุคคล	เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบเงื่อนไขเกี่ยวกับการประมวลผล ข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
ข้อแตกต่าง	PRIVACY POLICY	PRIVACY NOTICE												
สภาพบังคับทางกฎหมาย	กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)	กฎหมายกำหนดให้ผู้ควบคุมข้อมูล มีหน้าที่ต้องแจ้ง ตามมาตรา 23												
ขอบเขต	เป็นเอกสารที่สื่อสารถึงบุคคล ภายในองค์กร	เป็นประกาศที่มีผลเฉพาะ เจ้าของข้อมูลส่วนบุคคลเท่านั้น												
เนื้อหา	เป็นนโยบายและแนวปฏิบัติขององค์กร ในการคุ้มครองข้อมูลส่วนบุคคล	เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบเงื่อนไขเกี่ยวกับการประมวลผล ข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด												

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
2.3	Privacy Policy กับ Privacy Notice ต่างกันอย่างไร	Privacy Policy กับ Privacy Notice ต่างกันอย่างไร? PART 1 PRIVACY NOTICE ประกาศความเป็นส่วนตัว เป็นประกาศถึงเจ้าของข้อมูลส่วนบุคคลเพื่อแจ้งให้ทราบเกี่ยวกับรายละเอียดวิธีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงวิธีการดำเนินการต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคล โดยกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อนหรือขณะเก็บ รวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 PRIVACY POLICY นโยบายการคุ้มครองข้อมูลส่วนบุคคล เป็นนโยบายภายในองค์กรที่วางแนวปฏิบัติหรือกำหนด ทิศทางเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของบุคคลภายในองค์กรหรือหน่วยงานนั้น ๆ เพื่อให้สอดคล้อง กับหลักการและเงื่อนไขตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2.4	การเก็บรวบรวม ข้อมูลส่วนบุคคล	INFO 12/25 การเก็บรวบรวมข้อมูลส่วนบุคคล - เก็บรวบรวมได้เท่าที่จำเป็น ตามวัตถุประสงค์ อันชอบด้วยกฎหมาย - ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังนี้ - วัตถุประสงค์ของการเก็บรวบรวม - กรณีที่เราขอข้อมูลส่วนบุคคล ต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา - ข้อมูลส่วนบุคคลที่เราจะทำการเก็บรวบรวม และระยะเวลาในการเก็บรวบรวม - ประเภทของบุคคลหรือหน่วยงาน ซึ่งข้อมูลส่วนบุคคลนั้นเก็บรวบรวมอาจจะถูกเปิดเผย - ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานะผู้ติดต่อ และวิธีการติดต่อ - สิทธิของเจ้าของข้อมูลส่วนบุคคล ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 22 - 23)

3) หลักการขอความยินยอม

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
3.1	ความยินยอม	INFO 7/25 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ความยินยอม (Consent)  - ต้องได้รับความยินยอมก่อน หรือขอเก็บรวบรวมข้อมูลส่วนบุคคล - ต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์  - ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล - ต้องแยกส่วน ใช้ภาษาที่อ่านง่าย และไม่ใช่เป็นการหลอกลวง  - ความเป็นอิสระในการให้ความยินยอม - ถอนความยินยอมเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสุทธ ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 19)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
3.2	การขอความยินยอมจากผู้เยาว์	 การขอความยินยอมจากผู้เยาว์ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 20 กำหนดหลักการเกี่ยวกับความยินยอมของผู้เยาว์ ไว้ดังนี้ 1 ผู้เยาว์อายุ ไม่เกิน 10 ปี ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ 2 ผู้เยาว์อายุ ตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์ ต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ก่อน แต่บางกรณีผู้เยาว์ให้ความยินยอมเองได้ ดังนี้ 1) กรณีผู้เยาว์ทำการเพื่อไม่ให้เกิดสิทธิหรือเพื่อให้หลุดพ้นจากหน้าที่และต้องไม่มีเจตนาใด ๆ เช่น บริษัท ก ทำสัญญาให้ทุนการศึกษาแก่ผู้เยาว์ โดยไม่มีข้อผูกมัดหรือหน้าที่ใด จึงเป็นการทำนิติกรรมที่มีลักษณะเพียงเพื่อให้ไปซึ่งสิทธิในการศึกษา 2) กรณีผู้เยาว์ต้องแสดงเจตนาทำนิติกรรมเองโดยเป็นการเฉพาะตัวไม่อาจให้ผู้อื่นทำการแทน เช่น การทำนิติกรรมซึ่งผู้เยาว์สามารถกระทำได้เมื่อมีอายุ 15 ปีบริบูรณ์ 3) กรณีผู้เยาว์ทำการใด ๆ ซึ่งสมแก่ฐานะรูปแบบ และจำเป็นในการดำรงชีพ เช่น ผู้เยาว์สามารถสั่งซื้ออาหารออนไลน์ หรือเรียกรถรับจ้างผ่านแพลตฟอร์มเรียกรถโดยสารได้ด้วยตนเอง ตามประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์บรรลุนิติภาวะ เมื่อ (1) มีอายุครบ 20 ปีบริบูรณ์ หรือ (2) โดยการสมรสก่อนถึงวัยกฎหมาย
3.3	การขอความยินยอมจากคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ	 การขอความยินยอมจากคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ คนไร้ความสามารถ คือ บุคคลวิกลจริตที่ศาลสั่งให้เป็นคนไร้ความสามารถ ต้องขาดความรู้สึกละแวก ความรับผิดชอบอย่างรุนแรงทำการถึงส่วนตัวไม่ได้ ต้องอยู่ในความดูแลของผู้อนุบาลตามมาตรา 28 ของประมวลกฎหมายแพ่งและพาณิชย์ คนเสมือนไร้ความสามารถ คือ ผู้ที่ศาลได้สั่งให้เป็นคนเสมือนไร้ความสามารถ ต้องจัดอยู่ในความดูแลของผู้พิทักษ์ตามมาตรา 32 ของประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งมีลักษณะอย่างใดอย่างหนึ่งได้แก่ เป็นบุคคลมีกายพิการ หรือเป็นบุคคลมีจิตฟั่นเฟือนไม่สมประกอบ หรือเป็นบุคคลประพฤตีส่อสุรุยสุร่ายเสเพลเป็นอาชญา กรณีที่เจ้าพนักงานคุ้มครองข้อมูลส่วนบุคคลเป็น คนไร้ความสามารถ หรือ คนเสมือนไร้ความสามารถ ต้องขอความยินยอมจาก ผู้มีอำนาจกระทำการแทน ตามเงื่อนไขที่กฎหมายกำหนด

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
3.4	หลักความเป็นอิสระในการให้ความยินยอม	หลักความเป็นอิสระในการให้ความยินยอม ที่สอดคล้องกับหลักความอิสระของเจ้าของข้อมูลส่วนบุคคล กรณีตัวอย่าง.. - บัณฑิตโรงเรียน - “โรงเรียนต้องการใช้รูปนักเรียนสำหรับบัณฑิตโรงเรียน” ตัวอย่างความยินยอมที่มีความเป็นอิสระ: นักเรียนสามารถปฏิเสธการใช้ภาพถ่ายเหล่านั้นได้ โดยไม่มีความเสียหายใด ๆ เช่น ไม่ถูกปฏิเสธการศึกษาหรือการบริการ ตัวอย่างความยินยอมที่ไม่มีความเป็นอิสระ: นักเรียนถูกบังคับไม่ให้ทางตรงหรือทางอ้อมให้จำเป็นต้องยินยอมให้ใช้รูปถ่าย ที่มา : มาตรา 19 วรรคสี่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ
3.5	กรณีแบบไหนที่เรียกความอิสระในการให้ความยินยอม	กรณีแบบไหนที่เรียก “ความอิสระในการให้ความยินยอม” พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดให้ในการขอความยินยอม ต้องคำนึงถึงอย่างที่สุดในเรื่องความเป็นอิสระกับเจ้าของข้อมูลส่วนบุคคล โดยที่เจ้าของข้อมูลส่วนบุคคลมีทางเลือกที่แท้จริงในการให้ความยินยอม ผลของความยินยอมที่ไม่อิสระ: ความยินยอมนั้นไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างความยินยอมนั้นเป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ กล่าวคือ กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลนำความยินยอมหรือการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลในลักษณะเป็นการสร้างเงื่อนไขที่ไม่เกี่ยวข้องหรือจำเป็นสำหรับการให้บริการหรือสัญญา ดังเช่น วัตถุประสงค์เพื่อการตลาด และเจ้าของข้อมูลส่วนบุคคลไม่สามารถที่จะไม่ยอมรับได้ จึงเป็นความยินยอมโดยไม่อิสระ ที่มา : มาตรา 19 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
3.6	การประมวลผลข้อมูลส่วนบุคคลที่ต่างไปจากวัตถุประสงค์เดิม	
3.7	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
3.8	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA กรณีความยินยอม Consent ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รูปแบบการขอความยินยอม แต่จะต้องปรับให้เหมาะสมกับกิจกรรมการประมวลผลของตน เจ้าของข้อมูลมีสิทธิถอนเมื่อใดก็ได้ ทำโดยชัดแจ้งเป็นหนังสือ หรือผ่านระบบอิเล็กทรอนิกส์ก็ได้ ขอความยินยอมเท่าที่จำเป็นเฉพาะกรณีไม่มีการประมวลผลอื่น ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 และ 24 วรรคหนึ่ง *ฐานการประมวลผล หมายถึง การเก็บรวบรวมข้อมูลที่ได้รับยกเว้นตามมาตรา 24 และ 26

4) ฐานการประมวลผลที่ไม่ต้องขอความยินยอม

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
4.1	หลักการเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	หลักการเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA (Lawful Basis for Processing) 1 ความยินยอม Consent 2 ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ Vital Interest 3 ปฏิบัติตามสัญญา Contract 4 ประโยชน์สาธารณะ Public Task 5 จำเป็น/ชอบด้วยกฎหมาย Legitimate Interest 6 ปฏิบัติตามกฎหมาย Legal Obligations 7 เอกสารประวัติศาสตร์/วิจัย/สถิติ Research *เป็นกรณีเฉพาะ ครอบคลุมการประกาศกำหนด ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
4.2	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน	 INFO 11/25 การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) 6 Legal Obligations จำเป็นในการปฏิบัติตามกฎหมาย เฉพาะที่เกี่ยวข้องกับ Preventive or Occupational Medicine - เวชศาสตร์ป้องกันหรือเวชศาสตร์ - การประเมินความเสี่ยงด้านสุขภาพของลูกจ้าง - การวินิจฉัยโรคทางพันธุกรรม - การให้บริการด้านสุขภาพหรือด้านสังคม - การรักษาทางการแพทย์ การจัดการด้านสุขภาพ - หรือระบบของการให้บริการด้านสังคมสงเคราะห์ Public Health วิทยาการสาธารณสุขและการสาธารณสุข Health or Social Care Systems การคุ้มครองแรงงาน - การประกันสังคม หลักประกันสุขภาพแห่งชาติ - สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้สูงอายุตามกฎหมาย - การคุ้มครองผู้ประสบอันตราย หรือการคุ้มครองทางสังคม Archiving, Scientific or Historical Research - การศึกษาวินิจฉัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ - หรือประโยชน์สาธารณะอื่น Substantial Public Interest ประโยชน์สาธารณะที่สำคัญ ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 26)
4.3	การเก็บรวบรวม ข้อมูลส่วนบุคคลตาม PDPA	 การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA กรณีป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ Vital Interest เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล หรือเพื่อประโยชน์สาธารณะ เช่น ป้องกันโรคระบาด ผู้ควบคุมสามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม ข้อมูลส่วนบุคคลนั้นรวมถึงข้อมูลเกี่ยวกับชีวิต ร่างกาย หรือสุขภาพทุกประเภท - อุบัติเหตุ - การบริการทางการแพทย์ - การป้องกันโรคระบาด ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(2) และ 20(1) *การประมวลผล ได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
4.4	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA ปฏิบัติตามสัญญา ไม่ต้องขอความยินยอม Contract  เฉพาะข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอื่นใดไม่สามารถใช้ ฐานสัญญาได้*  เมื่อไม่ใช่เรื่องความยินยอม จึงไม่อาจถอนความยินยอมได้ เป็นเรื่องของนิติสัมพันธ์ตามสัญญา  จำกัดเฉพาะข้อมูลของเจ้าของข้อมูล ผู้เป็นคู่สัญญาเท่านั้น  ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่จำเป็น ในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเพื่อเข้าสู่สัญญา หรือเพื่อปฏิบัติตามสัญญา ก็ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลเพิ่มเติมอีก  ภายใต้ขอบเขตของสัญญา ตามที่ตกลงกัน ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3) *การปฏิบัติตามสัญญาไปเพียงพอที่จะนำไปเก็บรวบรวม ใช้ หรือเปิดเผยสำหรับข้อมูลอื่นใด เช่นแต่เป็นกรณีสัญญาให้บริการทางการแพทย์ที่เข้าเงื่อนไขตามกฎหมายตามมาตรา 26(5)(ก)
4.5	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA ปฏิบัติการของของรัฐ ไม่ต้องขอความยินยอม Public Task  หากจำเป็นต่อการดำเนินการของรัฐเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการนั้น ไม่ต้องขอความยินยอม  แม้ไม่ต้องขอความยินยอม แต่ผู้ควบคุมยังคงมีหน้าที่ในการ รักษาความปลอดภัยของข้อมูล  ดังนั้น ผู้ควบคุมข้อมูลจึงเป็นองค์กรของรัฐที่ปฏิบัติการตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่โดยอาศัยอำนาจที่ได้รับมอบหมายจากรัฐ  คำนึงถึงหลักความได้สัดส่วน ความจำเป็นในการใช้ข้อมูล และผลกระทบ ต่อความเป็นส่วนตัวของเจ้าของข้อมูล ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(4)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
4.6	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA ปฏิบัติตามกฎหมาย ไม่ต้องขอความยินยอม Legal Obligations จำเป็นสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมตามที่กฎหมายกำหนด หน้าที่ตามบทบัญญัติแห่งกฎหมาย หน้าที่ตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ  เช่น เก็บรวบรวม ใช้ หรือเปิดเผยเงินเดือนของลูกจ้างเพื่อส่งให้สำนักงานประกันสังคม ร้านค้าที่ให้บริการเชื่อมต่อ WiFi เก็บรวบรวมข้อมูลจากรถตามที่กำหนดในพ.ร.บ.คอมพิวเตอร์ ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(6)
4.7	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA กรณีจำเป็น/ชอบด้วยกฎหมาย Legitimate Interest จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น <u>โดยเจ้าของข้อมูลต้องสามารถคาดหมายได้</u> ผู้ควบคุมจึงต้องใช้ดุลยพินิจซึ่งนำหนักระหว่างประโยชน์อันชอบธรรมไม่ให้เกิดกับสิทธิและประโยชน์ของเจ้าของข้อมูล ไม่มีวิธีอื่นในการบรรลุวัตถุประสงค์ ผลประโยชน์อันชอบธรรมมีความชัดเจน  ประโยชน์อันชอบธรรม มีมาตรการปกป้องและคุ้มครองข้อมูล  สิทธิ/ประโยชน์ของเจ้าของข้อมูล มีความจำเป็นในการประมวลผล ไม่ส่งผลกระทบต่อเจ้าของข้อมูล ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5) *การประมวลผล หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
4.8	การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA	การประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการจ้างงาน ตัวอย่างกิจกรรม Lawful basis ที่อาจใช้ ก่อนการจ้าง การสมัครงาน → บ.24 (3) ระหว่างการจ้าง การใช้ข้อมูลส่วนบุคคลที่เกี่ยวข้องตามสัญญาจ้าง → บ.24 (3) การใช้ข้อมูลส่วนบุคคลอื่น ๆ ที่ไม่เกี่ยวข้องตามสัญญาจ้าง → ขึ้นอยู่กับกิจกรรม หลังสิ้นสุดสัญญาจ้าง ที่ทำงานใหม่ขอประวัติลูกจ้าง ที่ลาออกไปแล้ว → บ.24 โดยขอความยินยอมใช้ก่อนเลิกจ้าง หมายเหตุ : - เป็นข้อมูลส่วนบุคคลที่เก็บก่อน องค์กรอาจพิจารณาฐานอื่นตามความเหมาะสมที่สอดคล้องกับบทบัญญัติของกฎหมายได้ - ในการดำเนินการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 ต้องมีการพิจารณาตามมาตรา 26 ประกอบด้วย ที่มา : พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

5) สิทธิของเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.1	สิทธิของเจ้าของข้อมูลส่วนบุคคล	INFO 16/25 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right) - สิทธิได้รับการแจ้งให้ทราบ (Right to be informed) - สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access) - สิทธิขอโอนข้อมูลส่วนบุคคล (Right to data portability) - สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล (Right to object) - สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Right to erasure / Right to be forgotten) - สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing) - สิทธิขอแก้ไขข้อมูลส่วนบุคคล (Right to rectification) ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 และมาตรา 30 - 35 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.2	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิอะไรบ้าง	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิอะไรบ้าง ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สิทธิการได้รับแจ้ง (Right to be informed) มาตรา 23 สิทธิในการเพิกถอนความยินยอม (Right to Withdraw Consent) มาตรา 19 สิทธิการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) มาตรา 30 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification) มาตรา 35 และ 36 สิทธิในการลบข้อมูลส่วนบุคคล (Right to be Forgotten) มาตรา 33 สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (Right to Restrict of Processing) มาตรา 34 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right of Data Portability) มาตรา 31 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object) มาตรา 32 เป็นสิทธิพื้นฐานที่ทุกคนได้รับ วิธีการใช้สิทธิข้อ 2-8 เป็นไปตามที่กฎหมายกำหนด
5.3	สิทธิการได้รับแจ้งให้ทราบ	1.สิทธิการได้รับแจ้งให้ทราบ (Right to be Informed) มาตรา 23 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิอะไรบ้าง ต้องแจ้งวัตถุประสงค์ /รายละเอียด ในการประมวลผล* ผู้ควบคุมข้อมูล (DATA CONTROLLER) รู้ว่าคุณจะนำข้อมูลไปประมวลผลอย่างไร เจ้าของข้อมูลส่วนบุคคล (DATA SUBJECT) รายละเอียดการแจ้ง (Privacy Notice) - เก็บข้อมูลอะไร - ใช้เพื่ออะไร - เก็บนานแค่ไหน - ส่งต่อข้อมูลให้ใคร - ช่องทางการติดต่อ *หากเก็บข้อมูลจากแหล่งอื่น ก็ต้องแจ้งเจ้าของข้อมูลทราบด้วย (มาตรา 25) ถ้าไม่ปฏิบัติตาม จะมีโทษปรับสูงสุด 1,000,000 บาท (มาตรา 82) หากมีการแก้ไขวัตถุประสงค์ในภายหลัง ที่แตกต่างไปจากเดิม ต้องมีการแจ้งให้ทราบ *การประมวลผล หมายถึง การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 , มาตรา 25 , มาตรา 82

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.4	สิทธิในการเพิกถอน ความยินยอม	2. สิทธิในการเพิกถอนความยินยอม (Right to Withdraw Consent) มาตรา 19 1. แจ้งผลกระทบ 2. หยุดประมวลผล ผู้ควบคุมข้อมูล DATA CONTROLLER เจ้าของข้อมูลส่วนบุคคล DATA SUBJECT การเพิกถอน สามารถทำได้ตลอดเวลา โดยขั้นตอนจะต้องเข้าใจง่าย ไม่ซับซ้อน เฉพาะกรณีเก็บรวบรวมข้อมูล จากฐานความยินยอมเท่านั้น (มาตรา 19, 24, 26) หากไม่แจ้งผลกระทบจากการถอนความยินยอม จะมีโทษสูงสุด 1,000,000 บาท (มาตรา 82) - กรณีการร้องขอเพิกถอนความยินยอมโดยผู้เยาว์ ให้เป็นไปตามหลักเกณฑ์เกี่ยวกับการขอความยินยอม - การถอนความยินยอมไม่ส่งผลกระทบ ต่อการประมวลผลที่ให้ความยินยอมไปแล้ว *การประมวลผล หมายถึง การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19, มาตรา 82 กรมการส่งเสริมการค้าระหว่างประเทศ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
5.5	สิทธิการเข้าถึงข้อมูล ส่วนบุคคล	3. สิทธิการเข้าถึงข้อมูลส่วนบุคคล (Right of Access) มาตรา 30 ดำเนินการตามคำร้องขอภายใน 30 วัน ผู้ควบคุมข้อมูล DATA CONTROLLER เจ้าของข้อมูลส่วนบุคคล DATA SUBJECT 1. ขอบเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวข้อง 2. ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลของตนไม่ได้ให้ความยินยอม หากไม่ปฏิบัติตามคำขอ จะมีโทษสูงสุด 1,000,000 บาท (มาตรา 82) ผู้ควบคุมข้อมูลสามารถปฏิเสธคำขอได้ในกรณีดังต่อไปนี้ 1. ปฏิเสธตามกฎหมายหรือคำสั่งศาล 2. คำขอเป็นส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น *หากมีการปฏิเสธคำขอจะต้องทำบันทึกการปฏิเสธเกี่ยวกับการปฏิเสธด้วย (มาตรา 39) ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30, มาตรา 39 มาตรา 82 กรมการส่งเสริมการค้าระหว่างประเทศ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

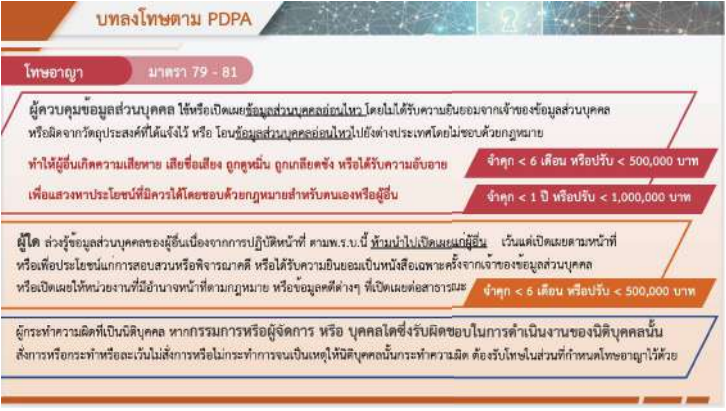
ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.6	สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	3. สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification) มาตรา 35, 36 อัปเดตข้อมูล และทำการแก้ไขให้ถูกต้อง เมื่อพบว่าข้อมูล ไม่ถูกต้องและไม่สมบูรณ์ สามารถแจ้งให้มีการแก้ไข “ข้อมูลส่วนบุคคล ถูกต้อง เป็นปัจจุบัน สมบูรณ์ ไม่ก่อให้เกิดความเข้าใจผิด” ผู้ควบคุมข้อมูล DATA CONTROLLER เจ้าของข้อมูลส่วนบุคคล DATA SUBJECT ในกรณีที่ผู้ควบคุมข้อมูลปฏิเสธคำร้องขอแก้ไขข้อมูล ให้บันทึกรายการและเหตุผลการปฏิเสธ ตามมาตรา 39 เมื่อถูกปฏิเสธการแก้ไข เจ้าของข้อมูลมีสิทธิร้องเรียน ต่อคณะกรรมการผู้ช่วยฯ เพื่อสั่งให้ผู้ควบคุมข้อมูลดำเนินการ ได้ตามมาตรา 34 วรรคสอง ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34, 35, 36, 37
5.7	สิทธิในการลบข้อมูลส่วนบุคคล	5. สิทธิในการลบข้อมูลส่วนบุคคล (Right to be Forgotten) มาตรา 33 “ลบ ทำลาย ทำให้ข้อมูลส่วนบุคคล ระบุดังตนไม่ได้” ผู้ควบคุมข้อมูล DATA CONTROLLER เจ้าของข้อมูลส่วนบุคคล DATA SUBJECT กรณีที่กฎหมายยกเว้นการใช้สิทธิ 1. ข้อมูลที่เกี่ยวข้องกับ เสรีภาพในการแสดงความคิดเห็น 2. ข้อมูลที่เกี่ยวข้องกับการทำวิจัย หรือเพื่อประโยชน์สาธารณะ 3. ข้อมูลที่กฎหมายระบุให้เก็บ ในกรณีเปิดเผยข้อมูลนั้น ต่อสาธารณะแล้ว ผู้ควบคุมข้อมูลต้องดำเนินการ แจ้งให้ลบข้อมูลดังกล่าวด้วย กรณีที่ผู้ควบคุมข้อมูล ไม่ดำเนินการตามคำร้องขอ เจ้าของข้อมูลมีสิทธิร้องเรียน ต่อคณะกรรมการผู้ช่วยฯ กรณีที่เจ้าของข้อมูลมีสิทธิ 1. ข้อมูลหมดความจำเป็นในการ ประมวลผลตามวัตถุประสงค์ 2. ทอนความยินยอมการใช้ข้อมูล 3. ข้อมูลถูกใช้ประมวลผล โดยไม่ถูกกฎหมาย *การประมวลผล หมายถึง การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24, มาตรา 33

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.8	การถอนความยินยอม	การถอนความยินยอม เมื่อเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมตามมาตรา 19 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว ก็สามารถถอนความยินยอมตามหลักการถอนความยินยอมตามมาตรา 19 วรรคห้า และมาตรา 19 วรรคหก ได้เช่นเดียวกัน จากหลักกฎหมายดังกล่าว สามารถแยกอธิบายเป็นประเด็นได้ ดังนี้ 1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะ ถอนความยินยอมเมื่อใดก็ได้ โดยร้องขอต่อผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นหน้าที่ของคณะกรรมการสิทธิฯ เช่น เจ้าหน้าที่ปฏิบัติการ หรือสายละเมิดฯ ฯลฯ และเจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมได้โดยง่าย เช่น การแจ้งการให้ความยินยอม 2 หลักการกีดกันการถอนความยินยอมตามมาตรา 19 วรรคห้า แบ่งเป็น 2 กรณี ได้แก่ 2.1 ข้อจำกัดสิทธิโดยกฎหมาย คือกรณีพิเศษ และ 2.2 ข้อจำกัดสิทธิโดยสัญญา คือกรณีทั่วไป การแจ้งการให้ความยินยอมและข้อจำกัดคือเป็นประโยชน์ต่อเจ้าของข้อมูลส่วนบุคคล 3 เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคล ไม่สามารถเก็บรวบรวม ใช้ เปิดเผย สำหรับกิจกรรมที่ถอนความยินยอมแล้ว และการถอนความยินยอมย้อนไปส่งผลต่อการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่ดำเนินการก่อนการถอนความยินยอมเป็นข้อ 4 ในกรณีการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ถึงผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรคหก Fig. 12-1
5.9	รู้หรือไม่เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ลบข้อมูลส่วนบุคคลได้	รู้หรือไม่? เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ลบข้อมูลส่วนบุคคลได้ (Right to Erasure) 1 เมื่อเจ้าของข้อมูลส่วนบุคคลมีความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 2 เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้วผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไป 3 เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 4 เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ - เว้นแต่ - 1. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น 2. การเก็บรักษาเพื่อวัตถุประสงค์เฉพาะ (เอกสารประวัติศาสตร์ / ประโยชน์สาธารณะ / วิชาชีพทางการแพทย์ / การสาธารณสุข ฯลฯ) 3. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ฯลฯ ตัวอย่าง นาย ก. สมัครใช้บริการของ บริษัท A ต่อมา นาย ก.เลิกสัญญา บริษัท A จึงหมดความจำเป็นในการปฏิบัติตามสัญญา นาย ก. จึงมีสิทธิขอให้ลบข้อมูลได้ เว้นแต่ บริษัท A ยังมีความจำเป็นต้องรักษาข้อมูลตามกฎหมายในการดำเนินงาน นาย ก. Fig. 24-1

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
5.10	หน้าที่ดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	 หน้าที่ดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล 1 ระยะเวลาดำเนินการ กรณีคำร้องขอเข้าถึงและขอรับสำเนา ให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ* 2 การให้เหตุผลในการปฏิเสธ สิทธิแต่ละประเภทมีเงื่อนไขและองค์ประกอบของการใช้สิทธิที่แตกต่างกัน เช่น สิทธิในการขอรับสำเนา อาจปฏิเสธคำขอได้ในกรณีเป็นการปฏิเสธตามกฎหมาย หรือคำสั่งศาล หรือการเข้าถึงหรือขอรับสำเนานั้นจะส่งผลกระทบต่อความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น* เป็นต้น 3 กระบวนการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ควรกำหนดเป็นนโยบายโดยระบุขั้นตอนการดำเนินงาน สำหรับจัดการและตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้กรอบที่กฎหมายกำหนด ให้ชัดเจน * ที่มา : มาตรา 30 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ
5.11	สิทธิขอแก้ไขข้อมูลให้ถูกต้อง	 สิทธิขอแก้ไขข้อมูลให้ถูกต้อง เจ้าของข้อมูลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลที่ไม่ถูกต้องของเจ้าของข้อมูลส่วนบุคคล เพื่อให้... ข้อมูลถูกต้องตรงกับข้อเท็จจริง ข้อมูลเป็นปัจจุบันและสมบูรณ์ ไม่ก่อให้เกิดความเข้าใจผิด หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลไว้ในบันทึกการกิจกรรมการประมวลผล (ROPA) * ที่มา : มาตรา 35 ประกอบมาตรา 36 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ

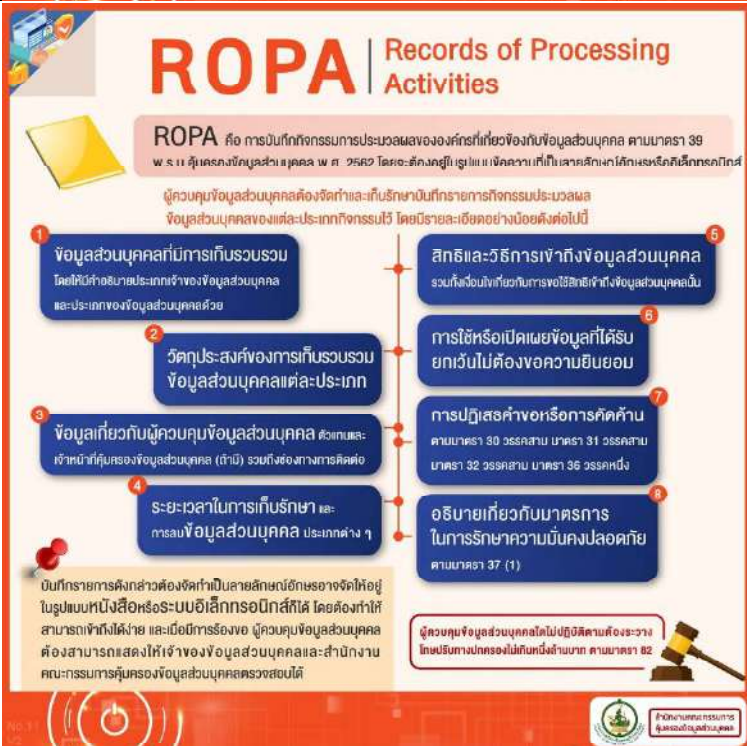
6) เหตุละเมิดข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
6.1	ความรับผิดทางแพ่ง	INFO 21/25 ความรับผิดทางแพ่ง ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกจากค่าสินไหมทดแทนที่ผู้ร้องแล้ว ศาลมีอำนาจสั่งให้จำคุกผู้ละเมิดเพื่อเป็นการลงโทษเพิ่มกันได้ แต่ไม่เกิน 2 ปี ของค่าสินไหมทดแทนที่ผู้ร้อง อายุความฟ้องคดี 3 ปี นับแต่วันที่ผู้เสียหาย ได้รับความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิดชอบ หรือ 10 ปี นับแต่วันที่การละเมิดข้อมูลส่วนบุคคล  ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 78) INFO 20/25 ความรับผิดทางแพ่ง ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องระงับค่าสินไหมทดแทน ไม่ว่าจะได้จากการกระทำโดยจงใจ หรือประมาทเลินเล่อหรือได้เกิดตาม เว้นแต่จะพิสูจน์ได้ว่า  ✓ เหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำ โดยเจ้าของข้อมูลส่วนบุคคล ✓ เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติ ตามหน้าที่และอำนาจตามกฎหมาย ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 79)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
6.2	โทษอาญา	 บทลงโทษตาม PDPA โทษอาญา มาตรา 79 - 81 ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามมาตรฐานทางจริยธรรมอย่างร้ายแรง โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากรหัสประสงค์ที่ได้แจ้งไว้ หรือ โยนข้อมูลส่วนบุคคลออกไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุก < 6 เดือน หรือปรับ < 500,000 บาท เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุก < 1 ปี หรือปรับ < 1,000,000 บาท ผู้ใด ละเมิดข้อมูลส่วนบุคคลของผู้ซึ่งเนื่องจากการปฏิบัติหน้าที่ ตามพ.ร.บ. นี้ ฐานล่วงละเมิดผู้อื่น เว้นแต่เปิดเผยตามหน้าที่ หรือเพื่อประโยชน์ในการสอบสวนหรือพิจารณา หรือได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือเปิดเผยให้นายงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือข้อมูลต่างๆ ที่เปิดเผยต่อสาธารณะ จำคุก < 6 เดือน หรือปรับ < 500,000 บาท ผู้กระทำความผิดที่เป็นนิติบุคคล หากกรรมการหรือผู้จัดการ หรือ บุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ละเว้นการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย
6.3	โทษทางปกครอง	 INFO 24/25 โทษทางปกครอง ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ☒ กระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด เช่น - ใต้แจ้งวัตถุประสงค์การเก็บรวบรวมข้อมูลส่วนบุคคล - ใต้แจ้งเจ้าของข้อมูลส่วนบุคคลทราบ - ขอลบข้อมูลโดยผิดกฏองเจ้าของข้อมูลส่วนบุคคล โทษปรับทางปกครองสูงสุด ไม่เกิน 5,000,000 บาท คณะกรรมการผู้เจ้าหน้าที่ มีอำนาจสั่งลงโทษปรับทางปกครอง

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
6.4	การร้องเรียน	
6.5	ตั้งค่า Website อย่างไรให้ลดการ ละเมิดข้อมูลส่วน บุคคล	

7) การเตรียมความพร้อมหรือแนวปฏิบัติ

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
7.1	Check list การเตรียมความพร้อมของหน่วยงาน	 Check list การเตรียมความพร้อมของหน่วยงาน ข้อกำหนดตามกฎหมาย Legal Compliance 1 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) บ.41 2 จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) บ.23 3 จัดทำบันทึกการกิจกรรมการประมวลผล (Records of Processing Activities) บ.39 4 จัดทำแบบขอความยินยอมในกรณีที่มีความจำเป็นต้องใช้ (Consent Form) บ.19 5 จัดทำข้อตกลงการประมวลผลในกรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) บ.40 ตัวอย่างแนวปฏิบัติที่ดี Best Practices 1 จัดตั้งคณะทำงาน PDPA ภายในหน่วยงาน (PDPA Working Team) 2 สำรองข้อมูลภายในหน่วยงานและจัดทำผังวงจรชีวิตข้อมูลส่วนบุคคล (Data Inventory) 3 จัดทำนโยบายและแนวปฏิบัติของหน่วยงาน (Privacy Policy and Codes of Practice) 4 ในกรณีที่มีการแบ่งปันหรือแลกเปลี่ยนข้อมูลระหว่างองค์กร ควรจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement) 5 สร้างความตระหนักและฝึกอบรม (Capacity Building and Awareness Raising) 6 ทำกับดูแลและตรวจสอบอย่างสม่ำเสมอ (Audit and Compliance) หมายเหตุ : นอกจาก Check list – การเตรียมความพร้อมนี้แล้วองค์กรยังมีหน้าที่อื่น ๆ ตามกฎหมายที่ต้องปฏิบัติตามด้วย
7.2	ROPA	 ROPA Records of Processing Activities ROPA คือ การบันทึกกิจกรรมการประมวลผลขององค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ตามมาตรา 39 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะบันทึกไว้ในระบบอิเล็กทรอนิกส์ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยรายละเอียดอย่างน้อยดังต่อไปนี้ 1 ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้คำอธิบายประเภทของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคลด้วย 2 วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท 3 ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตำแหน่งและเจ้าหน้าที่ที่ครอบครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ 4 ระยะเวลาในการเก็บรักษา และการลบข้อมูลส่วนบุคคล ประเภทต่าง ๆ 5 สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมถึงเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น 6 การใช้หรือเปิดเผยข้อมูลที่ได้รับ ยกเว้นไม่ต้องขอความยินยอม 7 การปฏิเสธคำขอหรือการคัดค้าน ตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม มาตรา 36 วรรคหนึ่ง 8 อธิบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1) บันทึกการดำเนินการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรหรือจัดให้อยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้เห็นเจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท ตามมาตรา 82

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
7.3	การเก็บรวบรวมข้อมูลส่วนบุคคลเกินความจำเป็นทำได้หรือไม่	 ท่านเก็บรวบรวมข้อมูลส่วนบุคคล เกินความจำเป็นหรือไม่? หลักการประมวลผลข้อมูลเท่าที่จำเป็น - Data minimization - ตามมาตรา 22 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ “การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล” เทียบเคียงได้กับ GDPR Article 5 (1) (5) อาจพิจารณาองค์ประกอบตาม GDPR ได้ดังนี้ 1 ข้อมูลส่วนบุคคลที่เก็บรวบรวมมี เพียงพอ (Adequate) ที่จะใช้ในการประมวลผลข้อมูลส่วนบุคคล 2 ข้อมูลส่วนบุคคลที่เก็บรวบรวมต้อง เกี่ยวข้อง (Relevant) กับการประมวลผลข้อมูลตามวัตถุประสงค์ 3 ข้อมูลส่วนบุคคลใช้อย่าง จำกัดเท่าที่จำเป็น (Limited) เพื่อให้บรรลุวัตถุประสงค์ของการเก็บรวบรวม ตัวอย่างเช่น เก็บรวบรวมข้อมูลชื่อ ที่อยู่ เบอร์โทรศัพท์ สำหรับวัตถุประสงค์ประสงค์ในการจัดส่งสินค้า จะเพียงพอ เกี่ยวข้อง และจำเป็นตามวัตถุประสงค์เพื่อจัดส่งสินค้าแล้ว ข้อควรคิด - ข้อมูลที่เก็บรวบรวมขึ้น มีส่วนในการทำให้บรรลุวัตถุประสงค์ของการเก็บข้อมูลหรือไม่ ? - หากไม่เก็บรวบรวมข้อมูลนั้นจะสามารถบรรลุวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้นได้หรือไม่ ? - มีทางเลือกอื่นในการเก็บรวบรวมข้อมูลน้อยกว่านี้เพื่อให้บรรลุวัตถุประสงค์ได้หรือไม่ ? ผู้ควบคุมข้อมูลส่วนบุคคลได้นำไปใช้/ใช้ตาม สังเกตว่าใช้ตามไม่ตรงกับ 3 ส่วนมาก ตามมาตรา 83 กรมส่งเสริมการค้าระหว่างประเทศ ศูนย์คุ้มครองข้อมูลส่วนบุคคล
7.4	ตัวอย่างการเก็บเอกสารที่อาจทำเพิ่มเติมเพื่อการปฏิบัติให้สอดคล้องกับกฎหมาย	 ตัวอย่างเอกสาร ที่อาจจัดทำเพิ่มเติม เพื่อการปฏิบัติให้สอดคล้องกับกฎหมาย 1 มาตรการเมื่อเกิดเหตุการณ์ละเมิดและกระบวนการแจ้ง (Data Breach Response and Notification Procedure) 2 แบบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต่อเจ้าของข้อมูลส่วนบุคคล (Data Breach Notification Form to Data Subjects) 3 รายละเอียดการะงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer Job Description) 4 แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request Form) 5 รายงานผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) 6 นโยบายระยะเวลาการจัดเก็บข้อมูล (Data Retention Policy) 7 นโยบายการทำลายข้อมูล (Data Disposal Policy) ที่มา มาตรา 23 (3), 37 (3), 37 (4), 39 (4), 39 วรรคท้าย, 41, 70 วรรคท้าย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กรมส่งเสริมการค้าระหว่างประเทศ ศูนย์คุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
7.5	6 ขั้นตอนพร้อมรับ DSRs	

8) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
8.1	DPO คือใคร	DPO คือใคร DPO (Data Protection Officer) คือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 42 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีหน้าที่ ดังนี้ - ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตาม พ.ร.บ. นี้ - ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล - ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล - รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มา เนื่องจากการปฏิบัติหน้าที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
8.2	พนักงานในบริษัทเป็น DPO ได้หรือไม่	พนักงานในบริษัทเป็น DPO ได้หรือไม่ เป็นได้ ใครเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO (Data Protection Officer) ได้อีก ? - DC (Data Controller) → พนักงานของ DC / Outsourced DPO - DP (Data Processor) → พนักงานของ DP / Outsourced DPO ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ - มาตรา 41 จรรยก้าย - " เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็น ผู้จ้างให้บริการตามสัญญา (outsourced DPO) กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล " - ข้อควรระวัง - อย่างไรก็ตาม ผู้ที่ทำหน้าที่เป็น DPO จะเป็นพนักงานก็ต้องทำหน้าที่ภายใต้กรอบงานหรือภาระงานนั้นๆ ต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
9.3	ประเภทของ Cookies	 ประเภทของ Cookies ตัวอย่างการแบ่งประเภทคุกกี้ของ UK ICO ซึ่งเป็นหน่วยงานคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร ได้จำแนกประเภทของคุกกี้ ออกเป็น 2 กลุ่ม 3 วิธีดังนี้* Our use of cookies We use necessary cookies to enhance your navigation, improve site usage, and enhance site navigation, improve site usage, and enhance site navigation. For more detailed information about the cookies we use, see our Cookies page. 1. คุกกี้ที่จำเป็น (Necessary cookies) คือ คุกกี้ที่จำเป็นเพื่อให้เว็บไซต์ทำงานได้และเป็นสิ่งจำเป็นที่ช่วยให้สามารถทำงานหลัก เช่น ความปลอดภัย การจัดการเครื่องช่วยและการช่วยเหลือสำหรับการเข้าถึง ผู้ใช้ อาจปิดใช้งานการตั้งค่าเหล่านี้ได้โดยการเปลี่ยนการตั้งค่าเบราว์เซอร์ของผู้ใช้ แต่อาจส่งผลต่อการทำงานของเว็บไซต์ 2. คุกกี้เพื่อการวิเคราะห์ (Analytics cookies) คือ คุกกี้ที่ช่วยจำและนับจำนวนผู้เข้าชมบนเว็บไซต์ และช่วยให้เจ้าของเว็บไซต์ทราบถึงพฤติกรรมในการเยี่ยมชมเว็บไซต์ เพื่อปรับปรุงการทำงานของเว็บไซต์ให้มีความดีขึ้น และมีความเหมาะสมมากขึ้น อีกทั้งเพื่อรวบรวมข้อมูลทางสถิติที่เกี่ยวกับวิธีการทำงาน เพื่อปรับปรุงการทำงานของเว็บไซต์โดยให้ผู้ใช้สามารถค้นหาสิ่งที่ต้องการได้อย่างง่ายดาย และช่วยให้เจ้าของเว็บไซต์สามารถปรับปรุงเว็บไซต์ *https://ico.org.uk/
9.4	วิธีการลบข้อมูล Cookies ของ Google chrome	 วิธีการลบข้อมูล Cookies ของ Google Chrome บุคคลสามารถจัดการและลบข้อมูลส่วนบุคคลของตนเองได้โดยการหมั่นตรวจสอบข้อมูล คุกกี้ใน Web Browser โดยในแต่ละ Web Browser จะมีวิธีการดำเนินการตั้งค่าที่แตกต่างกัน สำหรับ Google Chrome สามารถตั้งค่าได้ดังนี้ - คลิกที่เครื่องหมาย ... บนแถบด้านบนของเบราว์เซอร์ - คลิกที่ "Settings" - คลิกที่ "Privacy and Security" - คลิกที่ "Cookies and other site data" - ตั้งค่าตามความต้องการของผู้ใช้งาน 5.1 อนุญาตคุกกี้ทั้งหมด 5.2 ปิดกั้นคุกกี้ของบุคคลที่สามในบางเว็บไซต์แบบโปร-บุคคล 5.3 ปิดกั้นคุกกี้ของบุคคลที่สาม 5.4 ปิดกั้นคุกกี้ทั้งหมด 5.5 ล้างคุกกี้และข้อมูลอื่นที่เกี่ยวข้องเมื่อปิดหน้าต่างเว็บไซต์ทั้งหมด

10) แนวทางการป้องกันหรือมาตรการความปลอดภัย

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
10.1	มาตรการรักษาความมั่นคงปลอดภัย	 มาตรการรักษาความมั่นคงปลอดภัย ที่อาจนำมาใช้เพื่อให้อสอดคล้องกับ มาตรา 37 (1) กรณียตัวอย่าง NIST Cybersecurity Framework ของสหรัฐอเมริกา ซึ่งมีองค์ประกอบดังนี้ Identify การระบุและเข้าใจถึงระบบต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง Protect การวางมาตรฐานควบคุม เพื่อปกป้องระบบขององค์กร Detect การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ Respond การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น Recovery การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม ที่มา : NIST Cybersecurity Framework หรือ NIST CSF Version 1.1 เผยแพร่โดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกา
10.2	แนวทางการบริหารจัดการการเข้าถึงของผู้ใช้งาน	 แนวทางการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ตามมาตรฐาน ISO/IEC 27001 : 2013 เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและทรัพยากรโดยไม่ได้รับอนุญาต 1 การลงทะเบียนและการถอนสิทธิผู้ใช้งาน (User registration and de-registration) 2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning) 3 การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of privileged access right) 4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) 5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) 6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights) หมายเหตุ : เป็นเพียงข้อเสนอแนะเบื้องต้นเท่านั้น องค์กรอาจพิจารณาแนวทางอื่นเพื่อให้อสอดคล้องกับกติกบัญญัติของกฎหมายได้

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
10.3	กรณีใดบ้างที่ต้องลบข้อมูลส่วนบุคคล	

11) PDPA กับกรณีนอกราชอาณาจักร

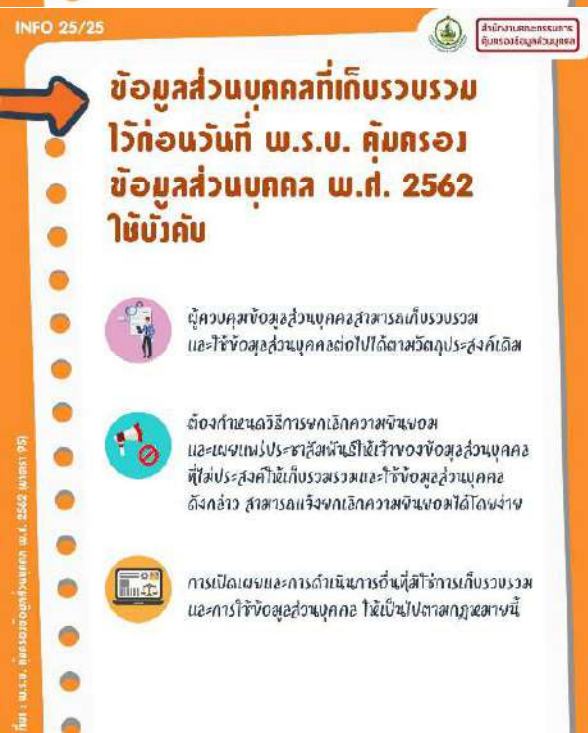
ลำดับ	ชื่อเรื่อง	ภาพประกอบ
11.1	การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
11.2	บริษัทตั้งอยู่ในประเทศไทยแต่เก็บข้อมูลของชาวต่างชาติจะต้องปฏิบัติตาม PDPA หรือไม่	บริษัทตั้งอยู่ในประเทศไทย แต่เก็บข้อมูลของชาวต่างชาติ จะต้องปฏิบัติตาม PDPA หรือไม่? พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลในราชอาณาจักร ไม่ว่าเจ้าของข้อมูลส่วนบุคคลจะมีสัญชาติใดก็ตาม ก็ยังคง ต้องปฏิบัติตามเงื่อนไขที่กฎหมายกำหนด ที่มา : มาตรา 5 วรรคแรก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ
11.3	กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่นอกราชอาณาจักรต้องปฏิบัติตาม PDPA	กรณีใดบ้าง ที่แม่ ผู้ควบคุม หรือ ผู้ประมวลผล ข้อมูลส่วนบุคคล ซึ่งอยู่นอกราชอาณาจักร ก็อาจ ต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เมื่อเป็นกิจกรรม ดังต่อไปนี้ ... 1 เสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม 2 การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร ที่มา : มาตรา 5 วรรคสอง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

12) เกร็ดความรู้อื่นๆ

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.1	ขอยกเว้นการใช้บังคับ พ.ร.บ.คุ้มครองข้อมูล ส่วนบุคคล	INFO 3/25 ขอยกเว้นการใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 1. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่ตั้งขึ้นโดยสภาผู้แทนราษฎร ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการพิจารณาขอขาน้ำดื่มและอาหาร ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการ แล้วยื่นต่อศาล 2. การพิจารณาพัฒนาผลิตภัณฑ์ของศาล และการดำเนินงานของเจ้าหน้าที่ ในการขอขาน้ำดื่มและอาหาร การบังคับคดี และการวางทรัพย์ รวมถึงการดำเนินงาน ตามกระบวนการยุติธรรมทางอาญา 3. การดำเนินการเกี่ยวกับข้อมูลของบริษัท ข้อมูลเครดิตและสิทธิการตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 4)
12.2	การเก็บรวบรวมข้อมูล ส่วนบุคคลจากแหล่งอื่น	INFO 13/25 การเก็บรวบรวมข้อมูลส่วนบุคคล จากแหล่งอื่น ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่... ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ โดยแจ้งให้ทราบ แต่ต้องไม่เกิน 30 วัน นับแต่วันที่ เก็บรวบรวมและได้รับความยินยอม จากเจ้าของข้อมูลส่วนบุคคล เป็นการเก็บรวบรวมข้อมูลส่วนบุคคล ที่ไม่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 25)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.3	การใช้หรือเปิดเผยข้อมูลส่วนบุคคล	INFO 14/25 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม เว้นแต่เป็นข้อมูลส่วนบุคคล ที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคล จากผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้น ไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคล ต้องบันทึกการใช้หรือเปิดเผยข้อมูลไว้ ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 27)
12.4	ขอบเขตการใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	INFO 1/25 ขอบเขตการใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร มีผลใช้บังคับ กับ กรณีผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมีกิจกรรม ดังนี้ เสนอขายสินค้าหรือบริการ แก่เจ้าของข้อมูลส่วนบุคคล ที่อยู่ในราชอาณาจักร ไม่ว่าจะด้วยการชำระเงินหรือไม่ก็ตาม เฝ้าติดตามพฤติกรรม ของเจ้าของข้อมูลส่วนบุคคล ที่เกิดขึ้นในราชอาณาจักร ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 5)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.5	ขอยกเว้นการใช้บังคับ พ.ร.บ.คุ้มครองข้อมูล ส่วนบุคคล	 INFO 2/25 ขอยกเว้นการใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของบุคคลที่ได้รับการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรม ในครอบครัวของบุคคลนั้นเท่านั้น 2. การดำเนินการของหน่วยงานของรัฐ ที่สืบเข้าในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการเมืองของรัฐ หรือการรักษาความปลอดภัย ของประชาชน รวมถึงหน้าที่เกี่ยวกับการ ป้องกันและปราบปรามการฉ้อโกง นิติวิทยาศาสตร์ หรือการรักษาความมั่นคง ปอลดลึงไซเบอร์ 3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผย ข้อมูลส่วนบุคคลที่ได้รับการเก็บรวบรวมไว้เฉพาะ เพื่อการสื่อสารมวลชน งานศิลปะกรรม หรืองานวรรณกรรมอันเป็นไปตามรัฐธรรมนูญ แห่งการประกอบวิชาชีพหรือเป็นประโยชน์ สาธารณะเท่านั้น ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 4)
12.6	ข้อมูลส่วนบุคคลที่เก็บ รวบรวมไว้ก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูล ส่วนบุคคล ใช้บังคับ	 INFO 25/25 ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับ - ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลต่อไปได้ตามวัตถุประสงค์เดิม - ต้องกำหนดวิธีการรักษาความมั่นคง และเผยแพร่ประชาสัมพันธ์ให้ไว้ว่าข้อมูลส่วนบุคคล ที่ไม่ประสงค์ให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ดังกล่าว สามารถแจ้งยกเลิกความมั่นคงได้โดยง่าย - การเปิดเผยและการดำเนินการอื่นที่สืบทอดการเก็บรวบรวม และการใช้ข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายนี้ ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 19)

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.7	พนักงานกับผู้ควบคุมข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พนักงาน ไม่ใช่ ในหน่วยงาน / องค์กร / สถาบัน ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) พนักงาน / ลูกจ้าง ทุกระดับ ไม่ว่าจะเป็นเจ้านายที่ ผู้จัดการ หรือผู้บริหาร แม้จะมีอำนาจตัดสินใจก็เป็นเพียงตัวแทน หรือผู้แทนที่กระทำการ ในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
12.8	พนักงานกับผู้ประมวลผลข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พนักงาน ไม่ใช่ ในหน่วยงาน / องค์กร / สถาบัน ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) พนักงานของนิติบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่กระทำตามคำสั่งหรือในนามของนิติบุคคลนั้น ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.9	พนักงานหรือส่วนงานในองค์กรเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่	พนักงานหรือส่วนงานในองค์กร เป็น ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล หรือไม่? HIGHLIGHTS - ในแต่ละองค์กร ผู้ควบคุมข้อมูลส่วนบุคคลคือองค์กรที่เป็นนิติบุคคล ไม่ใช่พนักงานหรือส่วนงานภายในองค์กร - สถานะ หน้าที่ และความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เป็นไปตามที่กฎหมายกำหนด ไม่สามารถมอบหมายไปยังบุคคลอื่น - พนักงานในบริษัทของสัญญาจ้างพนักงาน ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล Q & A Q พนักงานหรือส่วนงานในองค์กรจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแยกจากองค์กรหรือนิติบุคคลนั้น ๆ ได้หรือไม่ A พนักงานหรือส่วนงานในองค์กรถือเป็นส่วนหนึ่งขององค์กรที่ต้องปฏิบัติตามนโยบายและข้อกำหนดขององค์กรในส่วนของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น สอดคล้องกับบทบัญญัติของกฎหมาย ที่ต้องการกำหนดหน้าที่ความรับผิดชอบไว้ที่องค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและสอดคล้องกับแนวทางปฏิบัติสากล อาทิ ตาม EDPB Guidelines 07/2020 ที่ให้ข้อเสนอแนะที่ค่อนข้างเน้นกับใช้ GDPR ไว้ดังนี้ ในสถานการณ์ปกติ ผู้ควบคุมข้อมูลส่วนบุคคลย่อมหมายถึงองค์กรนั้น ๆ หากแต่สิ่งนี้ให้เหตุผลหรือส่วนงานใดควบคุมหรือดำเนินการเกี่ยวกับการประมวลผลใด ๆ ต้องถือว่าเป็นบุคคลที่ทำในนามขององค์กรเท่านั้น และไม่ทำให้บุคคลหรือส่วนงานเป็นนิติบุคคลเป็นลักษณะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่มา : EDPB Guidelines 07/2020 on the concept of controller and processor in the GDPR สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
12.10	หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล	หน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล Responsibilities of a Data Controller หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 37 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 - จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ - ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้รับใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ - จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือเจ้าของข้อมูลร้องขอ หรือเจ้าของข้อมูลได้ถอนความยินยอม - แจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้า ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อบุคคล และเสรีภาพของบุคคล ในกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อบุคคลและเสรีภาพของบุคคล ให้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย - ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร ต้องแต่งตั้งตัวแทนเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและต้องได้รับมอบอำนาจให้กระทำการแทนโดยไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการเก็บ รวบรวม หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล ** ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่อื่นที่ต้องดำเนินการ โดยมีรายละเอียดตามมาตราที่เกี่ยวข้อง ที่มา : EDPB Guidelines 07/2020 on the concept of controller and processor in the GDPR สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.11	หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล	 หน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล Responsibilities of a Data Processor กฎหมายกำหนดหน้าที่เฉพาะสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 มาตรา 40 ดังนี้ 1 ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. นี้ 2 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย โดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การเปิดข้อมูลส่วนบุคคลที่เกิดขึ้น 3 จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด 4 จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเฉพาะเมื่อเข้าเงื่อนไขที่มาตรา 41 กำหนด Warning! หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตาม ต้องระวางโทษปรับทางปกครองไม่เกิน 3 ล้านบาท สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
12.12	ข้อตกลงการประมวลผล หรือ DPA คืออะไร	 ข้อตกลงการประมวลผล หรือ DPA คืออะไร? หรือ DPA คืออะไร? ข้อตกลงการประมวลผล หรือ Data Processing Agreement (DPA) คือข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อกำหนด การดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบด้วยการแจ้งข้อมูลดังต่อไปนี้ 1 ต้องมีข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 2 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย 3 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล 4 มีข้อกำหนดเกี่ยวกับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การเปิดข้อมูลส่วนบุคคลที่เกิดขึ้น ข้อกำหนดทั้ง 4 ข้อเป็นกรอบเงื่อนไขเบื้องต้นที่ควรกำหนดไว้ ซึ่งรายละเอียดของเงื่อนไขสัญญา และข้อตกลงอื่นๆ เป็นเรื่องคู่สัญญาควรตกลงกันให้สอดคล้องกับกิจกรรมการประมวลผล และความถี่/หน้าที่ของข้อมูลและประสิทธิภาพของเจ้าของข้อมูลส่วนบุคคล ที่มา : มาตรา 40 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.14	ข้อตกลงระหว่างบุคคลที่เกี่ยวข้องกับ กิจกรรมการประมวลผล การประมวลผลข้อมูลส่วนบุคคล	 ข้อตกลงระหว่างบุคคลที่เกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ข้อตกลงแบ่งปันข้อมูล (Data Sharing Agreement (DSA)) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ข้อตกลงการประมวลผล (Data Processing Agreement (DPA)) หมายเหตุ : กรณีองค์กร A ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือกรณีตามมาตรา 24 หรือมาตรา 26 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ที่มา : พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ
12.15	เกร็ดความรู้เกี่ยวกับโทษอาญาในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ	 เกร็ดความรู้เกี่ยวกับโทษอาญาในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ ตาม GDPR นั้นจะไม่มีบทกำหนดโทษทางอาญา แต่คำปรับทางปกครองในอัตราที่สูงมาก เพราะว่า “การลงโทษทางอาญา” ไม่อยู่ในขอบอำนาจของสหภาพยุโรป ดังนั้น กฎหมายทุกฉบับที่เป็นกฎหมายของสหภาพยุโรป “จึงไม่มีโทษทางอาญา” แต่การกำหนดโทษอาญาเป็นอำนาจของรัฐสมาชิก ในประเทศเยอรมนีมีการตรา Federal Data Protection Act 2017 (BDSG) ขึ้น ก็มีการกำหนดโทษทางอาญาไว้ในมาตรา 42 โดยกำหนดโทษจำคุกไว้ไม่เกิน 3 ปีหรือปรับในกรณีที่กระทำความผิดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายกำหนด “PDPA สิงคโปร์ก็มีโทษทางอาญา” ซึ่งกำหนดความรับผิดทางอาญาไว้ 3 กรณี ได้แก่ 1 การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย 2 การใช้ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมายและทำให้ได้มาซึ่งผลประโยชน์หรือทำให้เกิดความเสียหายต่อบุคคล 3 การระบุตัวตนซ้ำ (re-identification) โดยไม่ชอบด้วยกฎหมาย ที่มา : General Data Protection Regulation (GDPR), Federal Data Protection Act 2017 (Bundesdatenschutzgesetz - BDSG), Personal Data Protection (Amendment) Act 2020 (No. 40 of 2020) (section 48D, 48E, 48F) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ชื่อเรื่อง	ภาพประกอบ
12.16	ข้อยกเว้นการบังคับใช้ PDPA สำหรับกิจการสื่อมวลชน	ข้อยกเว้นการบังคับใช้ PDPA สำหรับกิจการสื่อมวลชน ในกรณีกิจการสื่อมวลชน มาตรา 4 (3) เป็นข้อยกเว้นเชิงเนื้อหาที่ไม่ใช้บังคับตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่... 1 เป็นข้อยกเว้นเฉพาะ "กิจกรรมการประมวลผลข้อมูลส่วนบุคคล" ดังนั้นการประมวลผลที่ไม่เกี่ยวข้องกับการสื่อสารมวลชน กฎหมายไม่ได้ยกเว้น เช่น การใช้ข้อมูลพนักงาน การทำระบบสมาชิก เป็นต้น 2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ของกิจการสื่อมวลชนจะต้องเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น 3 ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับการยกเว้นยังคงต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ