การดำเนินการให้สอดคล้อง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

พ.ต.อ.สุรพงศ์ เปล่งขำ
ผู้อำนวยการ
สำนักตรวจสอบและกำกับดูแล

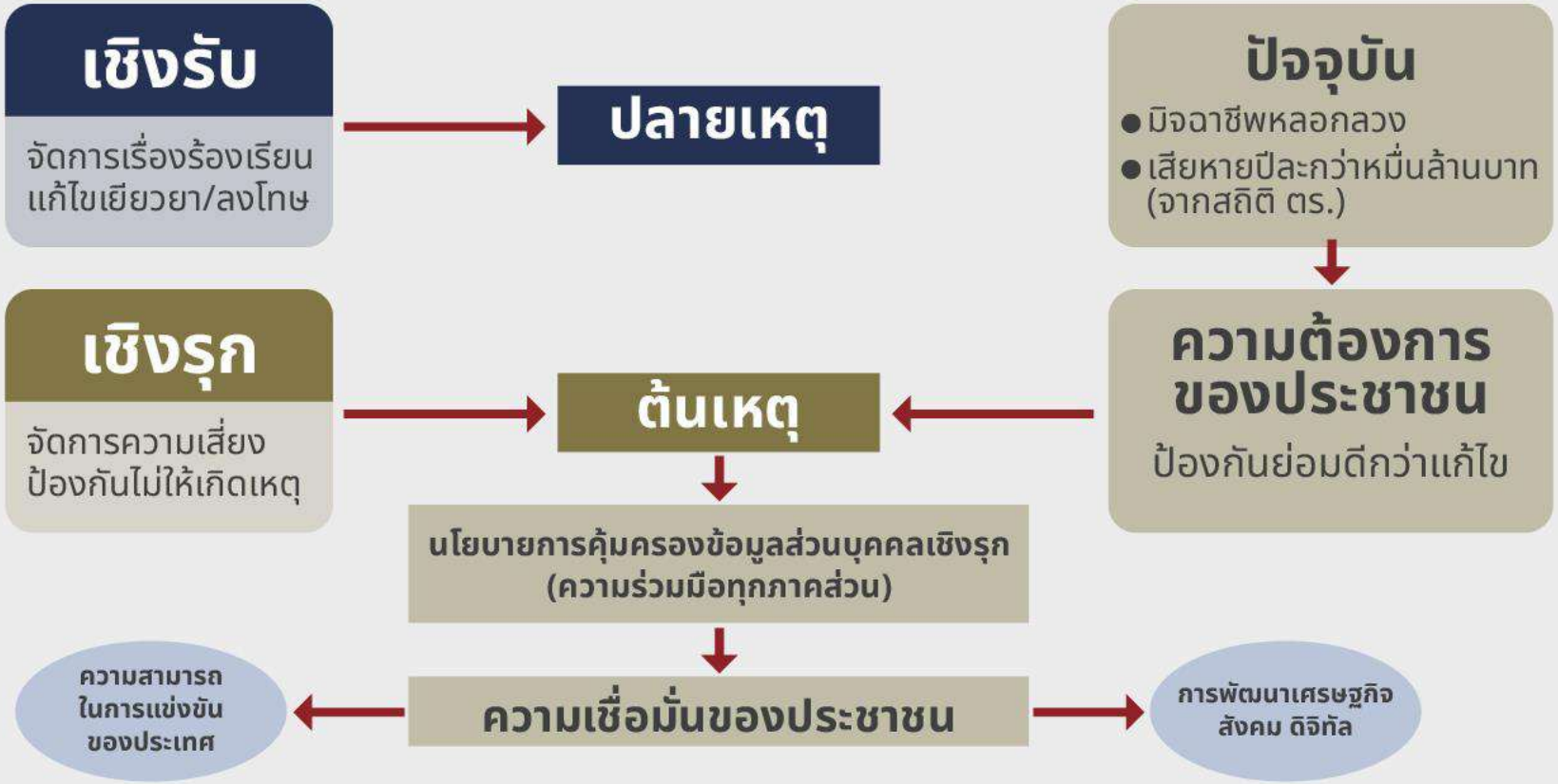
นายประสงค์ รุ่งแสง
ผู้อำนวยการฝ่าย
ตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล

ร.ท.ฐานันดร สำราญสุข
หัวหน้าศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล
(PDPC Eagle Eye)

นายกิตตินันท์ ศรีมงคล
ผู้อำนวยการฝ่าย
กำกับการคุ้มครองข้อมูลส่วนบุคคล

กลไกการขับเคลื่อนการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นหน่วยงานของรัฐ ที่มีหน้าที่และอำนาจตาม ม. 43 และ 44
ในการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศให้เป็นไปตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนด



ผลการดำเนินงานการเฝ้าระวังตรวจพบเหตุการละเมิดข้อมูลส่วนบุคคล

พฤศจิกายน 2566 – 31 กรกฎาคม 2567

ตรวจสอบแล้ว 31,561 หน่วย

ตรวจพบข้อมูลรั่วไหล 6,086 เรื่อง

แก้ไขแล้ว 6,081 เรื่อง

1. องค์กรปกครองส่วนท้องถิ่น	2,850 เรื่อง
2. ภาครัฐ	2,452 เรื่อง
3. การศึกษา	744 เรื่อง
4. ประกันภัย	21 เรื่อง
5. โทรคมนาคม	2 เรื่อง
6. สาธารณสุข	8 เรื่อง
7. การเงิน	4 เรื่อง

อยู่ระหว่างเร่งดำเนินการ 5 เรื่อง

ตรวจพบขายข้อมูล 139 เรื่อง

Facebook 109 เรื่อง
ปิดแล้ว 99 เรื่อง เฝ้าระวัง 10 เรื่อง

ขยายผล call center 7 เรื่อง
สอท. จับกุม 9 คน

เงินกู้นอกระบบ 1 เรื่อง
สอท. จับกุม 1 คน

เว็บพนันซื้อขายข้อมูล 1 เรื่อง
สอท. จับกุม 1 คน

ตรวจพบการเผยแพร่ข้อมูลส่วนบุคคล 21 เรื่อง
ตรวจพบบน กลุ่ม LOCK BIT 3.0 21 เรื่อง

ตรวจสอบสถานะเว็บซื้อขายข้อมูลส่วนบุคคล
BreachForums : สถานะ เปิด

รับแจ้งเหตุการละเมิด (สถิติ ณ 31 กรกฎาคม 2567

637 เรื่อง

ประเภทธุรกิจที่รับแจ้ง

การขนส่งและโลจิสติกส์	21	เรื่อง
การเงินการธนาคาร	262	เรื่อง
การศึกษา	29	เรื่อง
ค้าปลีกและค้าส่ง	42	เรื่อง
ท่องเที่ยวและกีฬา	5	เรื่อง
เทคโนโลยีสารสนเทศและโทรคมนาคม	33	เรื่อง
หน่วยงานของรัฐ-รัฐวิสาหกิจ	73	เรื่อง
ประกันภัย-ประกันชีวิต	47	เรื่อง
พลังงานและสาธารณูปโภค	3	เรื่อง
สาธารณสุข	29	เรื่อง
อสังหาริมทรัพย์	16	เรื่อง
อุตสาหกรรมการผลิต	39	เรื่อง
ด้านอื่นๆ	38	เรื่อง

สาเหตุการละเมิด

146	เปิดเผยเกินความจำเป็น	31	Hacker
246	Human Error	65	Threat
20	Google Search Engine	3	Social Media
37	เว็บไซต์ขายข้อมูล	5	Telegram
48	Malware Virus	33	อื่นๆ

การรวบรวมข้อมูล DPO (สถิติ ณ 31 กรกฎาคม 2567)

รวบรวมได้ทั้งหมด 2,173 หน่วยงาน

ภาครัฐ
125
หน่วยงาน

ภาครัฐที่ไม่เข้าข่าย มาตรา 41(1)
40 หน่วยงาน

มาตรา 41(1)
85 หน่วยงาน

ภาคเอกชน
2,048
หน่วยงาน

- ภาคเอกชนแต่งตั้งโดยสมัครใจ 1,026 หน่วยงาน
- มาตรา 41(2) 718 หน่วยงาน
- มาตรา 41(3) 86 หน่วยงาน
- มาตรา 41(2) และ มาตรา 41(3) 218 หน่วยงาน

หน้าที่ DPO มาตรา 42

ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ.นี้	จัดทำแผนการคุ้มครองข้อมูลส่วนบุคคลของหน่วยตน
ตรวจสอบการดำเนินการให้เป็นไปตาม พ.ร.บ.นี้	แบบตรวจแนะนำ 10 ด้านของ PDPC
ประสานงานและให้ความร่วมมือกับ PDPC	ประสานงานป้องกันและแก้ไขปัญหาตามแนวทางPDPC
รักษาความลับเนื่องจากการปฏิบัติตาม พ.ร.บ.นี้	ฝ่าฝืนเป็นความผิดตามมาตรา 80 มีโทษอาญา

การกำกับการคุ้มครองข้อมูลส่วนบุคคล

กพร. กำหนดตัวชี้วัด ให้ สคส. และ สกมช. ร่วมการตรวจแนะนำการกำกับข้อมูลส่วนบุคคล เพื่อลดการรั่วไหลของข้อมูลส่วนบุคคลของภาครัฐ

กำหนดตัวชี้วัดร่วมการตรวจแนะนำการกำกับคุ้มครองข้อมูลส่วนบุคคล 20 แห่ง ได้แก่

1. สำนักงานปลัดกระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์
2. กรมวิทยาศาสตร์การแพทย์
3. กรมการจัดหางาน
4. กองทุนเงินให้กู้ยืมเพื่อการศึกษา
5. คุรุสภา
6. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
7. การท่าพิเศษแห่งประเทศไทย
8. กรมพัฒนาชุมชน
9. สำนักงานปลัดกระทรวงศึกษาธิการ
10. ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย

มิถุนายน - กรกฎาคม 2567

11. กรมการกงสุล
12. กรมการท่องเที่ยว
13. สำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม
14. กรมท่าอากาศยาน
15. กรมพัฒนาฝีมือแรงงาน
16. กรมสุขภาพจิต
17. การประปาส่วนภูมิภาค
18. สำนักงานข้าราชการพลเรือน
19. มหาวิทยาลัยอุบลราชธานี
20. มหาวิทยาลัยมหาสารคาม

การกำกับการคุ้มครองข้อมูลส่วนบุคคล

การป้องกันและรับมือเหตุการละเมิดข้อมูลส่วนบุคคลทางไซเบอร์

- เพื่อสร้างโปรแกรมการจัดการความเป็นส่วนตัวที่ครอบคลุม (Privacy Program Management)
- เพื่อตรวจสอบแนวทางปฏิบัติที่มีอยู่ขององค์กรกับข้อกำหนดต่าง ๆ ใน PDPC Regulator Checklist
- เพื่อปรับปรุงแนวทางปฏิบัติที่มีอยู่ในบางข้อกำหนดหรือตัวชี้วัด
- เพื่อทำความเข้าใจวิธีการแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดของกฎหมายได้
- บันทึก ติดตามและรายงานความคืบหน้า หรือเพิ่มการมีส่วนร่วมของผู้บริหารระดับสูงและสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลทั่วทั้งองค์กร

กฎหมายลำดับรองที่ลงประกาศราชกิจจาฯ แล้ว

1	การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก	บังคับใช้ วันที่ 21 มิถุนายน 2565
2	มาตรการรักษาความมั่นคงปลอดภัยของ ผู้ควบคุมข้อมูลส่วนบุคคล	บังคับใช้ วันที่ 21 มิถุนายน 2565
3	หลักเกณฑ์มาตรการบังคับและพิจารณาลงโทษทางปกครอง	บังคับใช้ วันที่ 21 มิถุนายน 2565
4	การยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน	บังคับใช้ วันที่ 12 กรกฎาคม 2565
5	หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกิจกรรม การประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล	บังคับใช้ วันที่ 17 ธันวาคม 2565

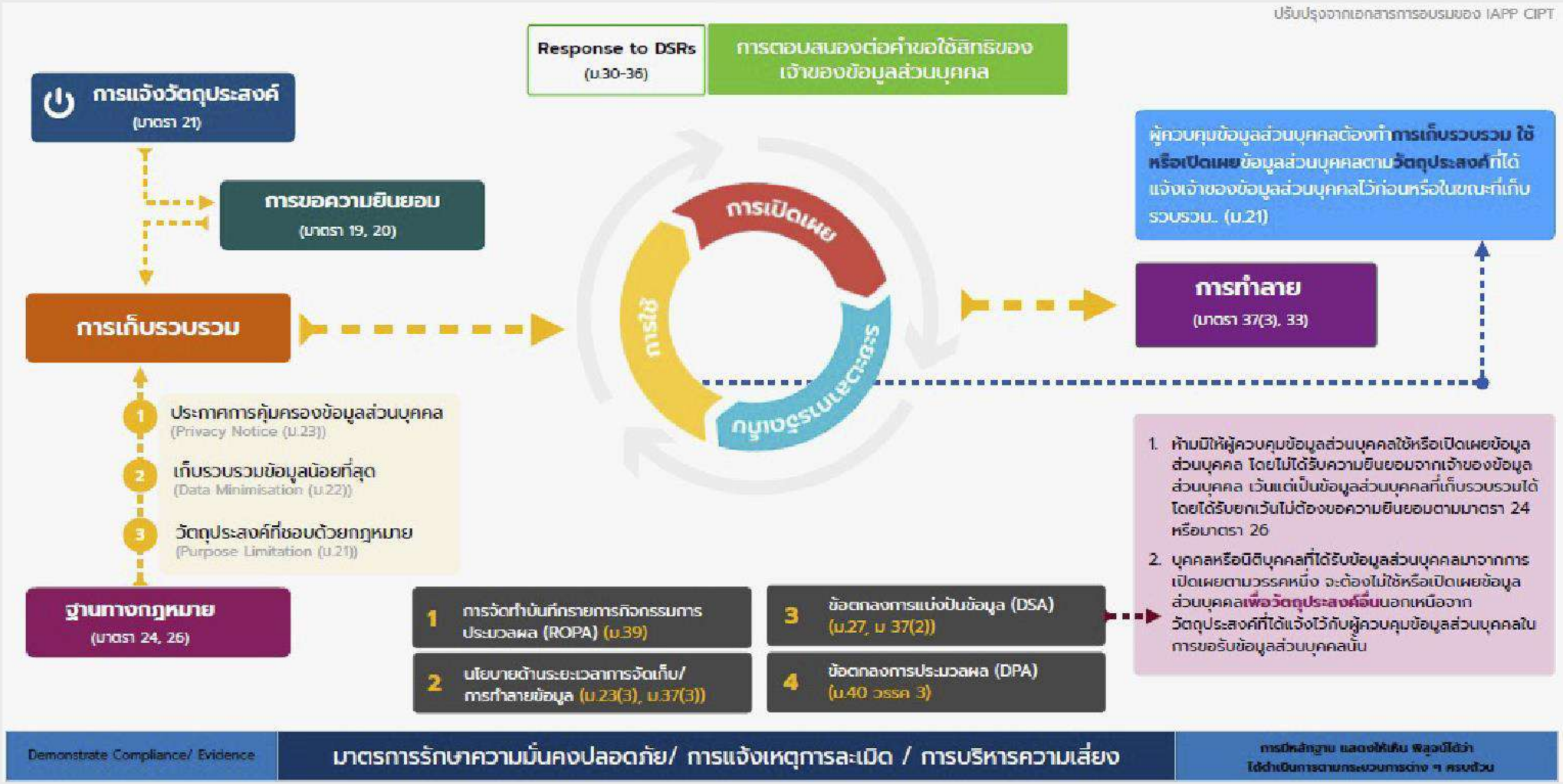
กฎหมายลำดับรองที่ลงประกาศราชกิจจาฯ แล้ว

6	หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	บังคับใช้ วันที่ 15 ธันวาคม 2565
7	หลักเกณฑ์และวิธีการในการจัดทำคำสั่งของคณะกรรมการผู้เชี่ยวชาญ	บังคับใช้ วันที่ 22 มิถุนายน 2566
8	ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	บังคับใช้ วันที่ 16 ตุลาคม 2566
9	การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	บังคับใช้ วันที่ 13 ธันวาคม 2566
10	พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงานที่ได้รับการยกเว้น ไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ	บังคับใช้ วันที่ 14 มกราคม 2567

กฎหมายลำดับรองที่ลงประกาศราชกิจจาฯ แล้ว

11	มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562มาใช้บังคับ	บังคับใช้ วันที่ 7 มีนาคม 2567
12	มาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวมข้อมูล ส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ รับฟังความเห็น มาตรา 24(1)	บังคับใช้ วันที่ 7 มีนาคม 2567
13	หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล ที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28	บังคับใช้ วันที่ 24 มีนาคม 2567
14	หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล ที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566	บังคับใช้ วันที่ 24 มีนาคม 2567
15	มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิต ตามมาตรา 26	บังคับใช้ วันที่ 7 เมษายน 2567
16	มาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	บังคับใช้ วันที่ 7 เมษายน 2567

ความเชื่อมโยง
การปฏิบัติตามกฎหมาย PDPA กับ “วงจรชีวิตข้อมูลส่วนบุคคล”



การดำเนินการของ PDPC

สำนักงานได้จัดทำแบบตรวจแนะนำ (Regulator Checklist)

เพื่อเป็นเครื่องมือในการกำกับดูแลให้แต่ละหน่วยงานสามารถนำมาตรการตามที่กฎหมายกำหนด ไปปฏิบัติได้อย่างเป็นรูปธรรมและมีประสิทธิภาพ ปรากฏตามตารางความสอดคล้อง

เป็นกลไกในการขับเคลื่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล,ประกาศ/ระเบียบ/แนวทางต่างๆที่ได้กำหนดไว้แล้วไปสู่การปฏิบัติจริง

ICO Framework Model → **กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)** ← ICO Framework Model

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล,ประกาศ/ระเบียบ/แนวทางที่กำหนดไว้แล้ว
1. ผู้นำและการกำกับดูแล	ม.41,42,ประกาศเรื่องหน่วยงานที่ต้องจัดให้มี DPO
2. นโยบายและแนวปฏิบัติ	ม.37,ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ
3. การอบรมและการสร้างความตระหนักรู้	ม.37,ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ4(7)
4. สิทธิของเจ้าของข้อมูลส่วนบุคคล	ม.19,23,30-36,73,ระเบียบว่าด้วยการยื่น...คำร้องเรียน,แนวทางการขอความยินยอม
5. การแจ้งวัตถุประสงค์และความโปร่งใส	ม.21,23,แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดฯ
6. การจัดทำบันทึกรายการและฐานทางกฎหมาย	ม.24,25,26,39,40,ประกาศเรื่องหลักเกณฑ์และวิธีการในการบันทึกรายการฯ
7. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล	ม.37(2),ม.40 วรรคสาม
8. ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	ม.19 วรรคหก,23(2),30 วรรคสอง,37(1)(4),39 วรรคสาม,40 วรรคสี่
9. มาตรการรักษาความมั่นคงปลอดภัย	ม.37(1),40(2), ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ
10. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	ม.37(4),ประกาศเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดฯ

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

1 ด้านผู้นำและการกำกับดูแล (Leadership and Oversight)

1. โครงสร้างองค์กร
2. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
3. การรายงานอย่างเหมาะสม
4. บทบาทการดำเนินงาน
5. ส่วนงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล
6. การประชุมกลุ่มปฏิบัติการ

ม.41, ม.42
ประกาศเรื่องหน่วยงาน
ที่ต้องจัดให้มี DPO

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

2 ด้านนโยบายและแนวปฏิบัติ (Policies and Procedure)

1. ทิศทางและการสนับสนุน
2. การทบทวนและอนุมัติ
3. การสร้างความตระหนักรู้ให้แก่พนักงาน
4. การคุ้มครองข้อมูลส่วนบุคคลในการออกแบบและดำเนินการ

ม.37
ประกาศเรื่องมาตรการรักษาความปลอดภัย

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

3 ด้านการอบรมและการสร้างความตระหนักรู้ (Training and Awareness)

1. โปรแกรมการสร้างความตระหนักและการฝึกอบรม
2. บทบาทพิเศษ
3. โปรแกรมการฝึกอบรม
4. การติดตามและประเมินผล
5. การสร้างความตระหนัก

ม.37
ประกาศเรื่องมาตรการรักษาความปลอดภัย
ข้อ4(7)

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

4 ด้านสิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual's Right)

1. การแจ้งสิทธิ
2. ทรัพยากร
3. การบันทึกการเข้าระบบและการติดตาม
4. การตอบสนองคำขอตามระยะเวลา
5. ข้อมูลที่ไม่ถูกต้อง
6. การติดตามและประเมินผลการปฏิบัติงาน
7. การโอนย้ายข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์
8. การลบ
9. การระงับ
10. การร้องเรียน
11. การประมวลผลโดยระบบอัตโนมัติ

ม.19,ม.23,ม.30-ม.36, ม.73
ระเบียบว่าด้วยการยื่น... ร้องเรียน แนวทาง การขอความยินยอม

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

5 ด้านการแจ้งวัตถุประสงค์และความโปร่งใส (Transparency)

1. รายละเอียดของประกาศการคุ้มครองข้อมูลส่วนบุคคล
2. จังหวะเวลาในการแจ้งวัตถุประสงค์
3. รายละเอียดเกี่ยวกับการแจ้งวัตถุประสงค์ที่มีประสิทธิภาพ
4. การตัดสินใจโดยระบบอัตโนมัติและการทำโปรไฟล์ลิ่ง
5. ความตระหนักรู้ของพนักงาน
6. การทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคล
7. เครื่องมือที่สนับสนุนความโปร่งใสและการควบคุม

ม.21,ม.23
แนวทางการดำเนินการ
ในการแจ้งวัตถุประสงค์
และรายละเอียดต่างๆ

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

6 ด้านการจัดทำบันทึกรายการและฐานทางกฎหมาย(ROPA and Lawful Basics)

1. องค์กรมีการจัดทำแผนผังข้อมูลที่ชัดเจน
2. องค์กรมีการจัดทำบันทึกรายการกิจกรรมครบถ้วนเป็นเอกสาร
3. บันทึกรายการกิจกรรมมีข้อมูลครบถ้วน
4. บันทึกรายการกิจกรรมมีการเชื่อมโยงข้อมูลไปยังเอกสารที่เกี่ยวข้อง
5. มีการกำหนดฐานทางกฎหมาย
6. การแจ้งวัตถุประสงค์และฐานทางกฎหมายให้ผู้ที่เกี่ยวข้องรับทราบ
7. ความยินยอมมีเงื่อนไขสอดคล้องกับมาตรา 19
8. การตรวจสอบและทบทวนความยินยอมที่ได้มาอย่างสม่ำเสมอ
9. องค์กรมีระบบในการตรวจสอบอายุและความสามารถของผู้เยาว์
10. สำหรับกรณีที่เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร

ม.24,ม.25,ม.26, ม.39,ม.40 ประกาศเรื่องหลักเกณฑ์และวิธีการในการบันทึกรายการฯ

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

7 ด้านข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล(DPA and DSA)

1. นโยบายและแนวปฏิบัติเกี่ยวกับการแบ่งปันข้อมูล
2. ข้อตกลงการแบ่งปันข้อมูล
3. การโอนข้อมูลส่วนบุคคลไปต่างประเทศ
4. ผู้ประมวลผลข้อมูลส่วนบุคคล
5. เงื่อนไขข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
6. การตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคล
7. การตรวจสอบการปฏิบัติตามสัญญา
8. การให้บริการโดยบุคคลที่สาม
9. วัตถุประสงค์ที่จำกัด

ม.37 (2),ม.40 วรรคสาม ระเบียบว่าด้วยการยื่น... ร้องเรียน แนวทาง การขอความยินยอม

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

8 ด้านความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Risks and DPIA)

1. การระบุ การบันทึก และการจัดการความเสี่ยง
2. องค์กรปกป้องข้อมูลโดยการออกแบบและกำหนดเป็นค่าเริ่มต้น
3. นโยบายและขั้นตอน DPIA
4. เนื้อหาของ DPIA
5. การลดและการทบทวนความเสี่ยงของ DPIA

ม.19 วรรคหก
ม.23 (2)
ม.30วรรคสองม.37 (1),(4)
ม.39 วรรคสาม
ม.40 วรรคสี่

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

9 ด้านมาตรการรักษาความมั่นคงปลอดภัย (Data Security)

1. การสร้าง การค้นหา และการเข้าถึงรายการข้อมูล
2. ความมั่นคงปลอดภัยสำหรับการถ่ายโอนข้อมูล
3. คุณภาพของข้อมูล
4. กำหนดระยะเวลาการจัดเก็บข้อมูล
5. การลบทำลายข้อมูล
6. บัญชีทรัพย์สินสารสนเทศ
7. ข้อกำหนดเกี่ยวกับการใช้ซอฟต์แวร์อย่างเหมาะสม
8. การควบคุมการเข้าถึง
9. การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
10. อุปกรณ์พกพาไร้สาย
11. พื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย
12. แผนความต่อเนื่องทางธุรกิจ การกู้คืนจากภัยพิบัติ และการสำรองข้อมูล

ม.37 (1),ม.40 (2) ประกาศเรื่องมาตรการรักษาความปลอดภัย

กรอบการตรวจแนะนำ 10 ด้าน (Regulator Checklist)

10 ด้านการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Response)

1. การตรวจพบ การบริหารจัดการ และการบันทึกเหตุการณ์
2. การประเมินและการรายงานเหตุการละเมิดข้อมูลส่วนบุคคล
3. การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ
4. การทบทวนและการเฝ้าระวังและติดตาม
5. การตรวจสอบโดยผู้ตรวจสอบภายนอก
6. โปรแกรมการตรวจสอบภายใน
7. ข้อมูลด้านประสิทธิภาพและความสอดคล้องกับข้อกำหนด
8. การใช้ข้อมูลเพื่อการจัดการ

ม.37 (4)
ประกาศเรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิด