ความท้าทายกฎหมายดิจิทัล ไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ที่ภาครัฐต้องใส่ใจ

บรรยายโดย

พันตำรวจเอกสุรพงศ์ เปล่งขำ

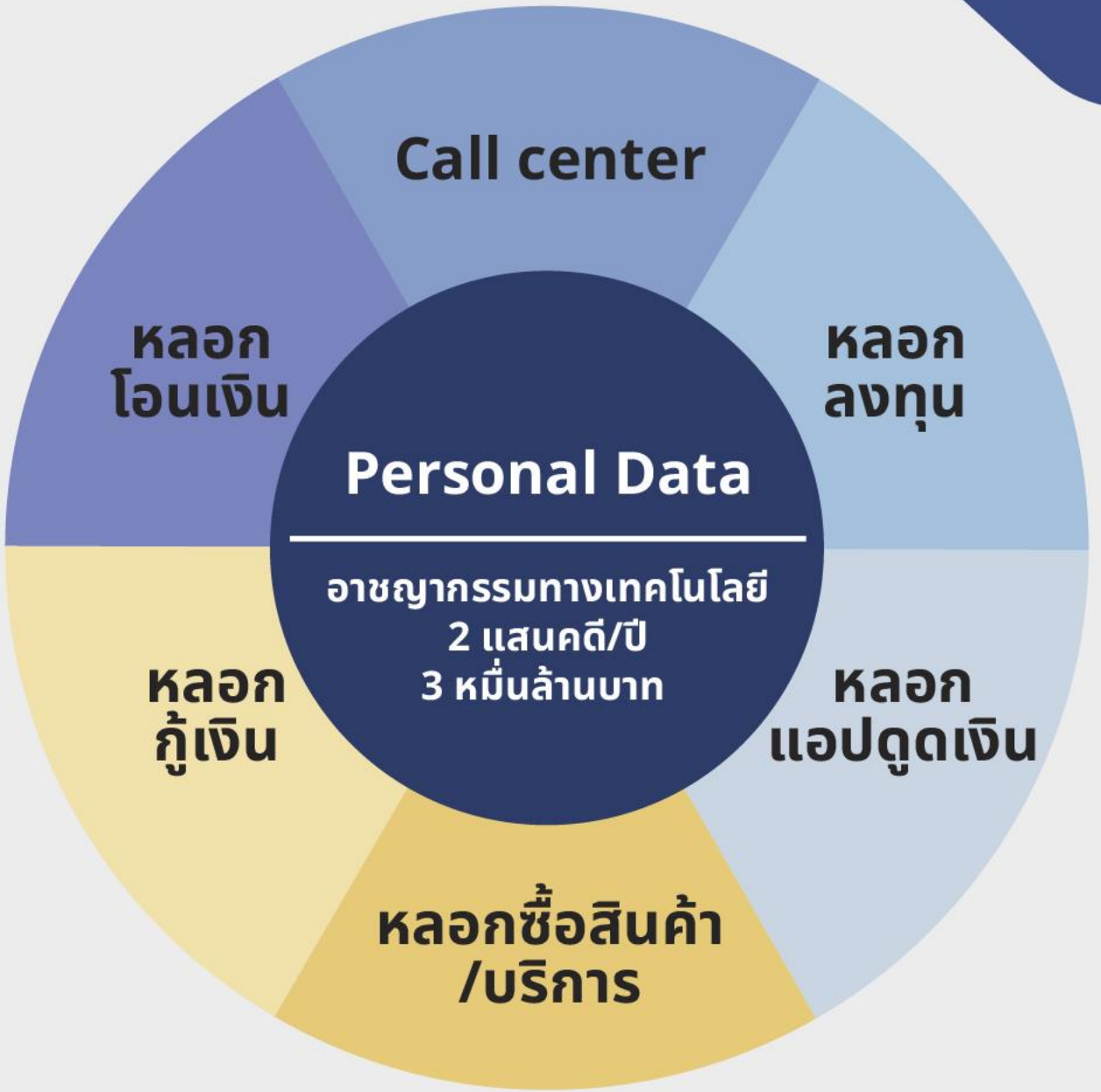
ผู้อำนวยการสำนักตรวจสอบและกำกับดูแล
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

Information Edge → Cyber Edge → Ai Edge

Convenient (ความสะดวก) & **Dangerous (ความอันตราย)**

control

พัฒนาการทางกฎหมาย


Call center
หลอก
โอนเงิน
หลอก
ลงทุน
Personal Data
อาชญากรรมทางเทคโนโลยี
2 แสนคดี/ปี
3 หมื่นล้านบาท
หลอก
กู้เงิน
หลอก
แอปดูดเงิน
หลอกซื้อสินค้า
/บริการ

EU และประเทศคู่ค้า

Laws

ประเทศไทย

GDPR
(General Data Protection Regulation) 2018
กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป

DSA
(Digital Service Act) 2024
กฎหมายให้บริการดิจิทัล
ควบคุม Platfrom ใหญ่
Facebook tiktok IG etc

DMA
(Digital Markets Act)2024
กฎหมายตลาดดิจิทัล

หลักคิด
"อะไรที่ผิดกฎหมายในโลก Offline
ก็ต้องผิดกฎหมายในโลก Online ด้วย"

PDPA
(Personal Data Protection Act) 2019
กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Cybersecurity Act 2019
กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์

พัฒนาการกฎหมายไทยที่เกี่ยวข้องกับดิจิทัลที่สำคัญ

- พ.ร.บ.ลิขสิทธิ์ พ.ศ.2537, 2558, 2561, 2565
- พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550, 2560
- พ.ร.บ.ว่าด้วยธุรกรรมทางอิเลคทรอนิกส์ พ.ศ.2544, 2551, 2562
- พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540
- พ.ร.บ.บริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ.2562
- พ.ร.บ.ปฏิบัติราชการทางอิเลคทรอนิกส์ พ.ศ.2565
- พ.ร.ก.มาตรการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566
- ประกาศคณะกรรมการบริหารศาลยุติธรรมจัดตั้งแผนกคดีอาชญากรรมทางเทคโนโลยีในศาลอาญา 19 มี.ค.2567

ตามมติคณะรัฐมนตรี

เมื่อวันที่ 21 พฤศจิกายน 2566

มาตรการป้องกันและคุ้มครองข้อมูลส่วนบุคคลของประเทศ

ระยะเร่งด่วน

จัดตั้ง

ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล (PDPC Eagle Eye)

- เร่งตรวจสอบ ค้นหา เฝ้าระวัง การรั่วไหลของข้อมูลเพื่อระงับยับยั้ง ไม่ให้เกิดความเสียหายที่อาจเกิดขึ้น โดยเร็ว
- สร้างความตระหนักรู้ด้านการป้องกันและคุ้มครองข้อมูลส่วนบุคคล ร่วมกับหน่วยงานที่เกี่ยวข้อง และ DPO

การดำเนินงานของศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล (PDPC Eagle Eye)

ผลการดำเนินงาน (6 เดือน) เดือนพฤศจิกายน 2566 – เดือนเมษายน 2567

ตรวจสอบแล้ว 25,063 หน่วย

ตรวจพบข้อมูลรั่วไหล 5,963 เรื่อง

แก้ไขแล้ว 5,953 เรื่อง

1. องค์กรปกครองส่วนท้องถิ่น	2,832 เรื่อง
2. ภาครัฐ	2,411 เรื่อง
3. การศึกษา	679 เรื่อง
4. ประกันภัย	21 เรื่อง
5. โทรคมนาคม	2 เรื่อง
6. สาธารณสุข	5 เรื่อง
7. การเงิน	3 เรื่อง

อยู่ระหว่างเร่งดำเนินการ 10 เรื่อง

ตรวจพบขายข้อมูล 83 เรื่อง

Facebook 75 เรื่อง
ปิดแล้ว 65 เรื่อง

ขยายผล call center 7 เรื่อง
สอท. จับกุม 9 คน

เงินกู้นอกระบบ 1 เรื่อง
สอท. จับกุม 1 คน

สาเหตุที่ตรวจพบและแนวทางแก้ไข

จากผลการตรวจพบการรั่วไหลของข้อมูลส่วนบุคคล

สาเหตุ/ความเสี่ยง	แนวทางแก้ไข
 เปิดเผยเกินความจำเป็น	X5 (Masking) การพรางข้อมูล
 Human Error	ป้องกันโดยมาตรการเชิงองค์กร การควบคุมและกำกับดูแล แบบตรวจ 10 ด้าน (PDPC Regulators Checklist)
 Google Search	ป้องกันโดย Encryption การเข้ารหัส
 ตรวจพบมากที่สุด	สร้างความตระหนักรู้และกำกับดูแล

นายประเสริฐ จันทรรวงทอง
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

การสร้างความตระหนักรู้ที่สำคัญ

งานขับเคลื่อนนโยบายป้องกันและคุ้มครองข้อมูลส่วนบุคคล แก่ องค์กรปกครองส่วนท้องถิ่น

เมื่อวันที่ 22 กุมภาพันธ์ 2567

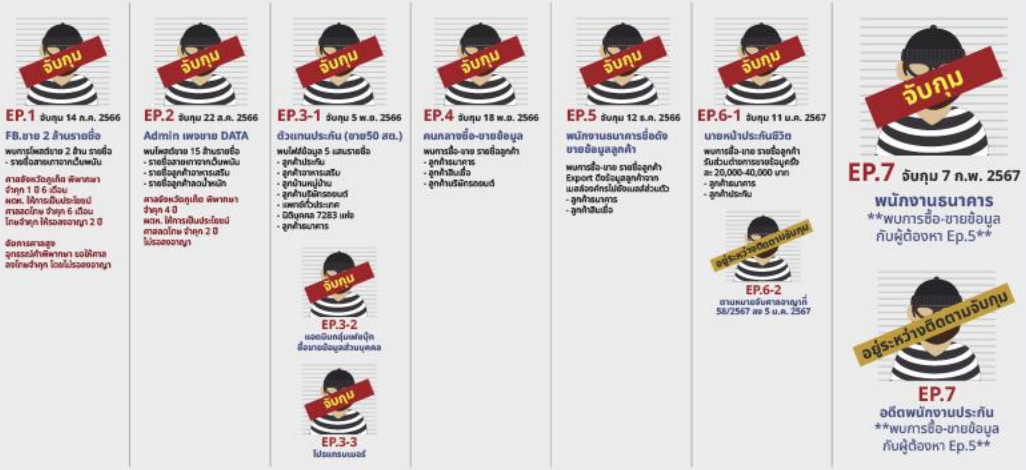
76 จังหวัด
7,850 หน่วย

โดยรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานในการจัดงานและมอบนโยบาย 4 ข้อ

1. ไม่ควรเปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น
2. แต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล
3. กำกับดูแลให้เป็นไปตามกฎหมายที่เกี่ยวข้อง
4. ให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามแผนจัดการสัมมนาถ่ายทอดความรู้

การขยายผลกรณีตรวจพบขายข้อมูล

ขยายผล call center 7 เรื่อง
สอท. จับกุม 9 คน



ขยายผลเงินกู้นอกระบบ 1 เรื่อง
สอท. จับกุม 1 คน

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

8 พ.ค.67 สำนักงาน ก.พ.ร. ได้จัดประชุมชี้แจงกรอบและแนวทางการประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชน โดย ท่าน วิริยา เนตรน้อย รองเลขาธิการ ก.พ.ร. ได้ยกตัวอย่างหน่วยงาน ที่มีการดำเนินงานการบูรณาการร่วมกัน การร่วมดำเนินงานเพื่อสร้างประโยชน์ให้กับประชาชน หรือ Impact กับประเทศชาติ ได้อย่างเห็นผล ซึ่งเป็นเป้าหมายของการจัดตั้งองค์การมหาชน ซึ่งทาง ก.พ.ร. จะนำผลการดำเนินงานของ 2 หน่วยงานไปเป็น Base Practice ให้กับหน่วยงานอื่นต่อไป

การตรวจพบข้อมูลรั่วไหล มีสัดส่วนที่ลดลง

สรุปสถิติผลการดำเนินการป้องกันและคุ้มครองข้อมูลส่วนบุคคลเชิงรุก ตามมติ ครม. ระหว่างวันที่ 9 พ.ย. 2566 ถึง 30 เม.ย. 2567
ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล (PDPC Eagle Eye) ผลการตรวจ 25,063 หน่วย

	ผลการตรวจ	ตรวจพบข้อมูลรั่วไหล	แก้ไขแล้ว	รอดำเนินการ	สัดส่วนข้อมูลรั่วไหล
พ.ย. 2566	7,290	2,289	2,289	0	31.40
ธ.ค. 2566	6,074	1,454	1,454	0	23.94
ม.ค. 2567	5,895	1,271	1,271	0	21.56
ก.พ. 2567	3,154	564	564	0	17.88
มี.ค. 2567	1,401	231	225	6	16.49
เม.ย. 2567	1,249	154	150	4	12.33
	25,063	5,963	5,953	10	23.79

31.40

สัดส่วนลดลง

12.33

5,963

1	องค์กรท้องถิ่น	2,832 เรื่อง	5	โทรคมนาคม	2 เรื่อง
2	รัฐ	2,411 เรื่อง	6	สาธารณสุข	5 เรื่อง
3	การศึกษา	679 เรื่อง	7	การเงิน	3 เรื่อง
4	ประกันภัย	21 เรื่อง			

ผลสัมฤทธิ์จากการสร้างความตระหนักรู้

ป้องกัน

สร้างความตระหนักรู้ DPO Network
แบบตรวจ 10 ด้าน
(PDPC Regulators Checklist)

มอบนโยบาย
DPO ภาครัฐ
ณ 16 พ.ย.66

เครือข่าย DPO
ณ 9 พ.ย.66
ภาครัฐ 85 หน่วยงาน

ป้องกัน

สร้างความตระหนักรู้
DPO Network
แบบตรวจ 10 ด้าน
(PDPC Regulators
Checklist)

- เครือข่ายธุรกิจประกันภัย 1 ธ.ค.66
- เครือข่าย อปท. ทั่วประเทศ 22 ก.พ.67
- ตรวจแนะนำการกำกับดูแลร่วม สกมช.
- MOU กับหน่วยงานรัฐและเอกชน

เครือข่าย DPO เพิ่มขึ้นเป็น 2,216 หน่วยงาน

ภาครัฐ
124
หน่วยงาน

ภาครัฐที่ไม่เข้าข่าย มาตรา 41(1)
39 หน่วยงาน

มาตรา 41(1)
85 หน่วยงาน

ภาคเอกชน
2,092
หน่วยงาน

- ภาคเอกชนแต่งตั้งตัวแทนสนักรใจ 1,046 หน่วยงาน
- มาตรา 41(2) 749 หน่วยงาน
- มาตรา 41(3) 88 หน่วยงาน
- มาตรา 41(2) และ มาตรา 41(3) 209 หน่วยงาน

ผลสัมฤทธิ์จากการสร้างภูมิคุ้มกันให้สังคม

ผนึกกำลัง สร้างภูมิคุ้มกันให้สังคม

แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. 2567-2570

กำหนดให้มีการบูรณาการความร่วมมือภาครัฐและเอกชนในการขับเคลื่อนแผนแม่บท

ยุทธศาสตร์ที่ 1 การเพิ่มประสิทธิภาพการบังคับใช้กฎหมาย PDPA Effective and Balanced Enforcement

ยุทธศาสตร์ที่ 2 การพัฒนากำลังคนและสร้างความเชื่อมั่น PDPA Knowledge and Trust Enhancement

ยุทธศาสตร์ที่ 3 การส่งเสริมเศรษฐกิจและสังคมดิจิทัล PDPA Digital Economy and Society Promotion

ยุทธศาสตร์ที่ 4 การสนับสนุนระบบนิเวศวิจัยและส่งเสริมการใช้เทคโนโลยี PDPA R&D and Technology Adoption

1. ด้านความมั่นคงภาครัฐ
2. ด้านบริการภาครัฐที่สำคัญ
3. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
4. ด้านการขนส่งและโลจิสติกส์
5. ด้านพลังงานและสาธารณูปโภค
6. ด้านสาธารณสุข
7. ด้านการศึกษา
8. ด้านการเงิน การลงทุน และการประกัน
9. ด้านการท่องเที่ยว
10. ด้านการค้าส่ง-ค้าปลีก และการค้าออนไลน์
11. ด้านอสังหาริมทรัพย์

ผลสัมฤทธิ์จากการขับเคลื่อนการคุ้มครองข้อมูลส่วนบุคคลเชิงรุก

มาตรการคุ้มครองเชิงรุก	ผลลัพธ์	แผนการดำเนินการขั้นต่อไป
ป้องปราม PDPC Eagle Eye	การตรวจพบข้อมูลรั่วไหล มีสัดส่วนที่ลดลง	ยกระดับ → ขับเคลื่อนนโยบายการคุ้มครองข้อมูลส่วนบุคคลเชิงรุกอย่างต่อเนื่อง
ป้องกัน สร้างความตระหนักรู้ DPO Network แบบตรวจ 10 ด้าน (PDPC Regulators Checklist)	เครือข่าย DPO เพิ่มขึ้น	
พนึกกำลัง สร้างภูมิคุ้มกันให้สังคม	แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. 2567-2570	ยกระดับ → บูรณาการความร่วมมือภาครัฐและเอกชนในการขับเคลื่อนแผนแม่บทอย่างเป็นรูปธรรม

การกำกับการคุ้มครองข้อมูลส่วนบุคคล

กลไกการกำกับการคุ้มครองข้อมูลส่วนบุคคล

PDPC
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่และอำนาจ

"กำกับดูแลทุกหน่วยงานในภาพรวมของประเทศ"

มาตรา 43

"ดำเนินการให้เป็นไปตามวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล"

มาตรา 44(10)

"ติดตามและประเมินผลการปฏิบัติตาม พ.ร.บ. นี้"

การดำเนินการ

- จัดทำแผนการตรวจแนะนำ
- จัดทำแบบตรวจแนะนำ
- การประสานงานป้องกันและแก้ไขปัญหาก่อนเกิดเหตุ/ขณะเกิดเหตุ/หลังเกิดเหตุ

DPO
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หน้าที่

"กำกับดูแลหน่วยงานของตน"
ตามมาตรา 42

(1) ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ.นี้
(2) ตรวจสอบการดำเนินการให้เป็นไปตาม พ.ร.บ.นี้
(3) ประสานงานและให้ความร่วมมือกับ PDPC
(4) รักษาความลับเนื่องจากการปฏิบัติตาม พ.ร.บ.นี้

เครือข่าย DPO

การคุ้มครอง
เข้มแข็ง
ทั่วถึง
มีประสิทธิภาพ

~~โอกาส~~

- เหตุการละเมิด
- ข้อมูลรั่วไหล
- การคุกคามอื่นๆ

การกำกับการคุ้มครองข้อมูลส่วนบุคคล

การป้องกันและรับมือเหตุการละเมิดข้อมูลส่วนบุคคลทางไซเบอร์

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

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

นโยบาย
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

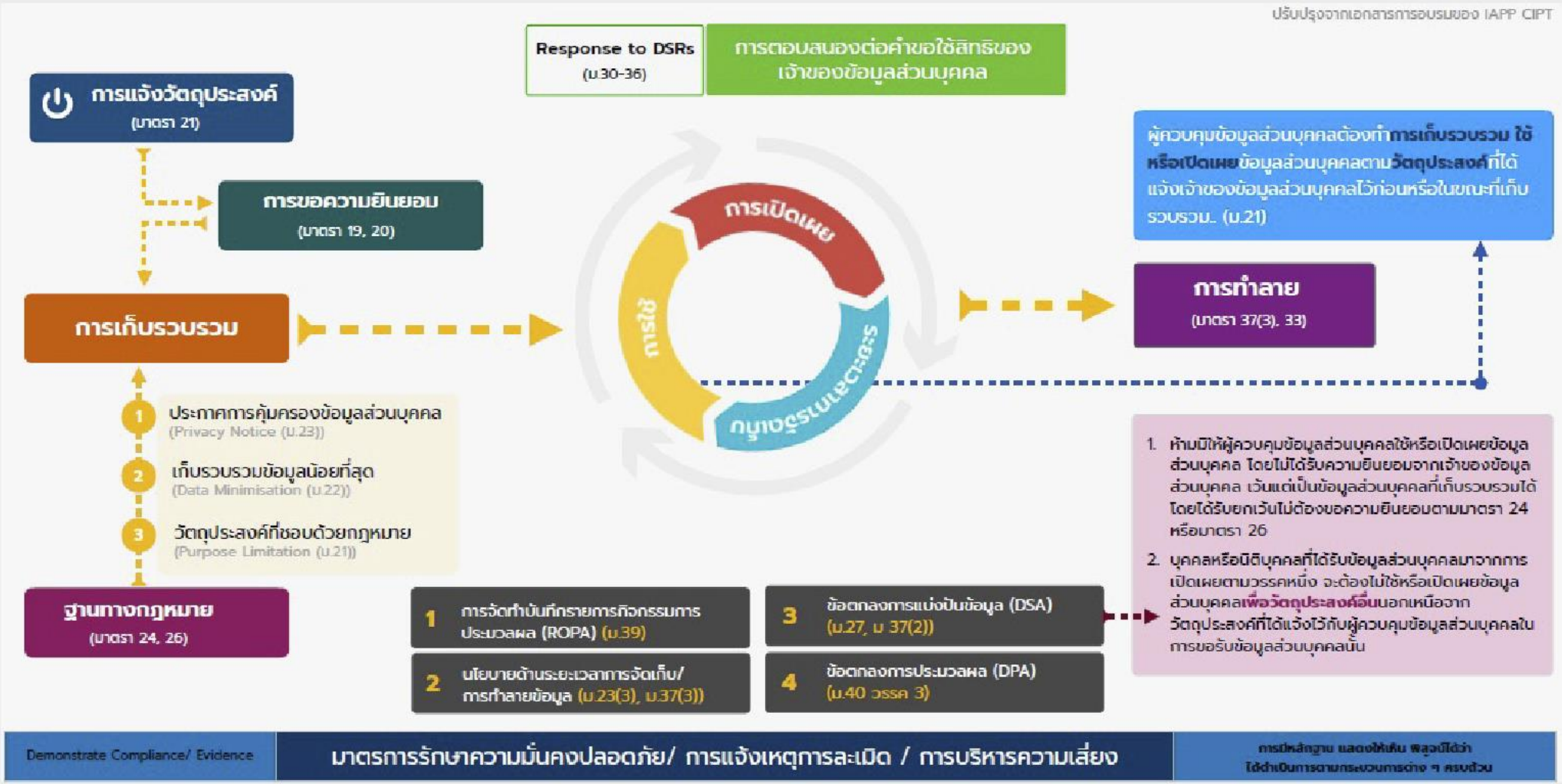
ได้มอบนโยบายแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ในการประชุมเครือข่ายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ครั้งที่ 1/2566 เมื่อวันที่ 16 พฤศจิกายน 2566 สรุปสาระสำคัญ ดังนี้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเปรียบเสมือน
"Super Hero ผู้คุ้มครองข้อมูลส่วนบุคคลของประชาชน"

จึงขอให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทุกท่าน มุ่งมั่นตั้งใจปฏิบัติหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลของประชาชน ให้ปลอดภัยจากมิจฉาชีพและภยันตรายต่างๆ ดังต่อไปนี้

1. ตรวจสอบและดูแลให้หน่วยงานของตนมีการปฏิบัติตามกฎหมาย PDPA อย่างเคร่งครัด
2. ตรวจสอบเฝ้าระวังไม่ให้มีข้อมูลส่วนบุคคลของประชาชนรั่วไหลบนเว็บไซต์และช่องทางอื่นๆ
3. ตรวจสอบไม่ให้มีการเก็บรวบรวมหรือเผยแพร่ ข้อมูลส่วนบุคคลของประชาชนมากเกินความจำเป็น
4. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยสำหรับเข้าถึงข้อมูลส่วนบุคคล อาทิการพิสูจน์ยืนยันตัวตน กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูลฯ
5. จัดให้มีมาตรการกำกับดูแลเจ้าหน้าที่ภายในหน่วยงานไม่ให้มีการนำข้อมูลส่วนบุคคลของประชาชนไปขาย หรือเปิดเผยโดยมิชอบ
6. จัดให้มีการฝึกอบรมเพื่อสร้างองค์ความรู้และความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลให้แก่เจ้าหน้าที่ภายในหน่วยงาน

ความเชื่อมโยง
การปฏิบัติตามกฎหมาย PDPA กับ “วงจรชีวิตข้อมูลส่วนบุคคล”



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

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