สำนักงาน ก.ล.ต.

ถอดบทเรียนการดำเนินการ ด้านการคุ้มครองข้อมูลส่วนบุคคล ของสำนักงาน ก.ล.ต.

การดำเนินการด้าน PDPA ภายในสำนักงาน (As of 30 เมษายน 2564) ภาพรวมความคืบหน้า 96.4 %

1 90%
จัดทำแผนผังข้อมูลส่วนบุคคล

(5W +1H)
: อยู่ระหว่างจัดทำ (Q2/64) สถานะ 90%

- มีการจัดทำทะเบียนที่ระบุถึงข้อมูลส่วนบุคคล ที่ปฏิบัติตาม PDPA แล้ว
- มีการจัดทำ Data flow ที่เป็นต้นแบบแล้ว เช่น flow การให้ความเห็นชอบบุคลากร

2 ☑ กำหนดหน้าที่ของบุคคลและฐานกฎหมาย

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ประมวลข้อมูลส่วนบุคคล : หน้าที่ในการเก็บรวบรวม ใช้ เปิดเผย
การโอนไปยังต่างประเทศ : ไปยังบริษัทภายในและบุคคลภายนอก
ฐานทางกฎหมาย : ความยินยอม หรือข้อยกเว้นอื่นตามกฎหมาย

3 ☑ จัดทำเอกสารที่จำเป็นต้องใช้

เอกสารทางกฎหมาย : จัดทำสัญญาและนโยบายต่างๆ
การนำไปใช้ : ลูกค้า พนักงาน เจ้าของข้อมูลที่มีอยู่เดิม เจ้าของข้อมูลใหม่

4 ☑ บริหารจัดการข้อมูลตาม Data life cycle +กำหนดสิทธิ

ขั้นตอนการปฏิบัติงาน ; การบริหารจัดการวงจรชีวิตข้อมูล และการจัดการเกี่ยวกับสิทธิเจ้าของข้อมูล

5 85%
จัดทำระบบ IT เพื่อรองรับตาม PDPA

ระบบเทคโนโลยีและการตรวจสอบ : มาตรการรักษาความปลอดภัยสารสนเทศและเครื่องมือ
: อยู่ระหว่างจัดทำ และทดสอบ
- ข้อมูลเดิมที่สำนักงาน
ฝ่าย ICT ได้จัดทำระบบ แจ้ง privacy policy ของสำนักงาน ให้เจ้าของข้อมูลทราบ (ทาง website , ทาง email) อยู่ระหว่างทดสอบและนำเสนอสำนักงาน
- ข้อมูล ongoing
อยู่ระหว่างฝ่าย ICT พัฒนาระบบงาน เพื่อรองรับการแจ้ง consent , privacy policy

6 ☑ แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล(DPO)

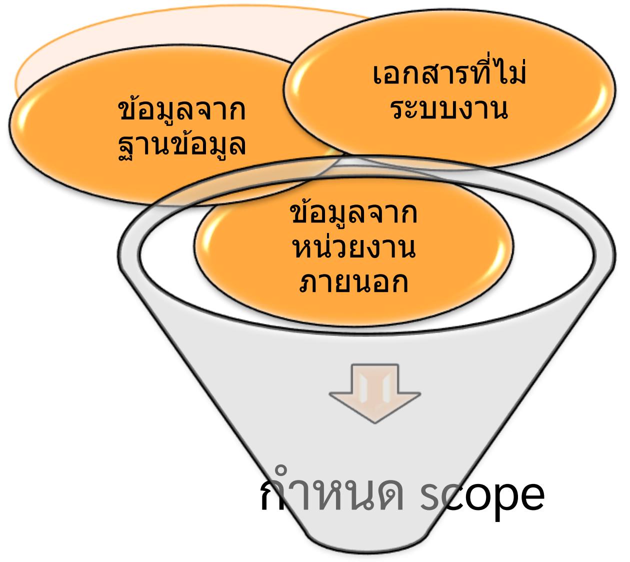
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและตัวแทน : DPO และ DPO Office

7 ☑ จัดอบรมและสร้างความตระหนักรู้

การอบรมและการสร้างความตระหนักรู้
: ผ่านหลักสูตร Online ของนิติจุฬาตรวจสอบ เสร็จแล้ว พร้อมส่ง 100%
: ประชาสัมพันธ์ ผ่าน Infographic จัดทำเสร็จแล้ว 100% อยู่ระหว่างเตรียมรูปแบบประชาสัมพันธ์

จัดทำแผนผังข้อมูลส่วนบุคคล

1 กำหนด scope + ระบุชุดข้อมูลส่วนบุคคล

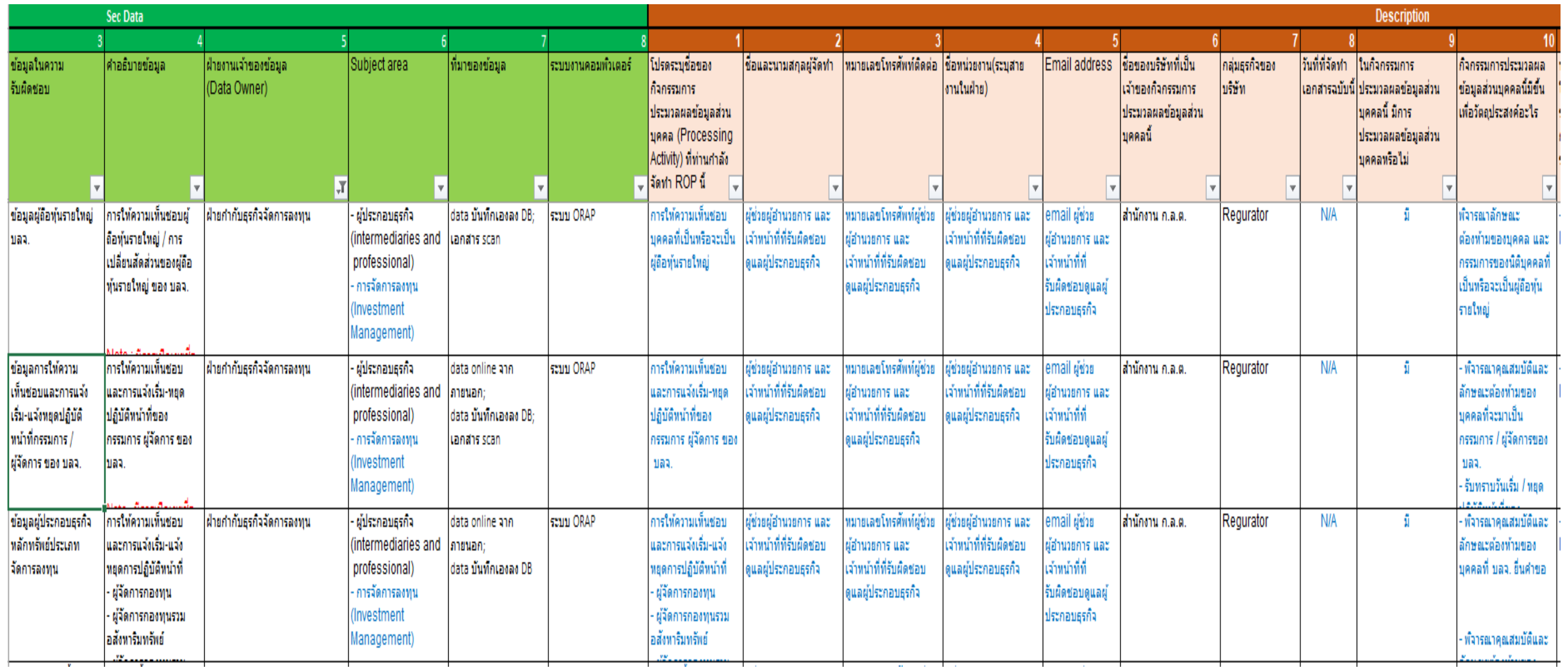


+

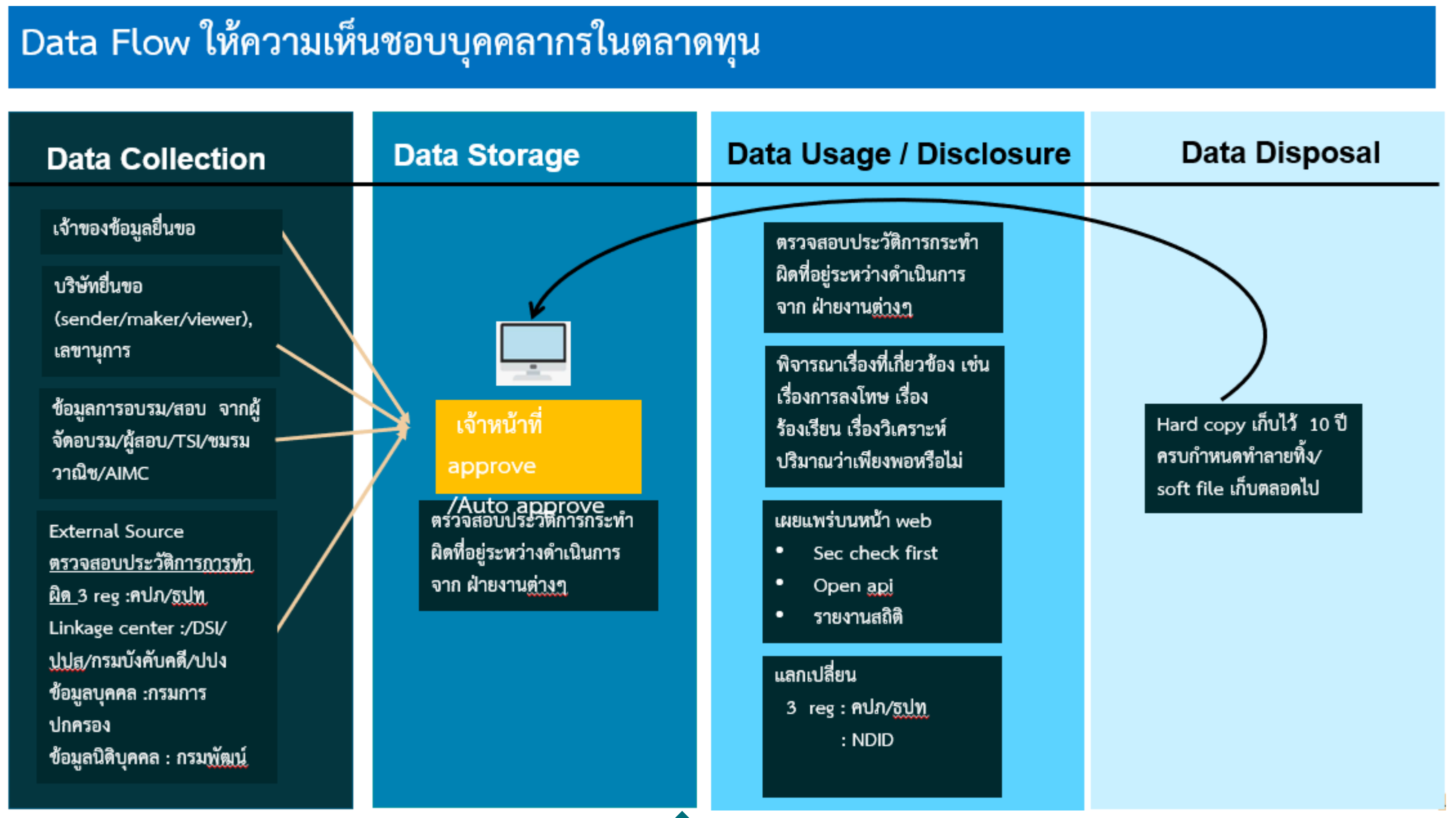
ลำดับ	ข้อมูล	Confidential data	Direct identifier	Indirect identifier	Sensitive data
1	เลขที่บัตรประชาชน / เลขที่หนังสือเดินทาง		√		
2	ชื่อ-นามสกุล (ไทย + อังกฤษ)		√		
3	วันเกิด			√	
4	สัญชาติ			√	
5	เบอร์โทรศัพท์มือถือ		√		
6	email		√		
7	ที่อยู่ตามบัตรประชาชน			√	
8	การศึกษา			√	
9	เพศ			√	√
10	สถานภาพการสมรส			√	√
11	ประวัติการกระทำความผิด			√	√

2 จัดทำทะเบียน :ROP

- Description
- Collection
- Storage
- Usage
- Transfer
- Disposal
- Access Control
- Encryption

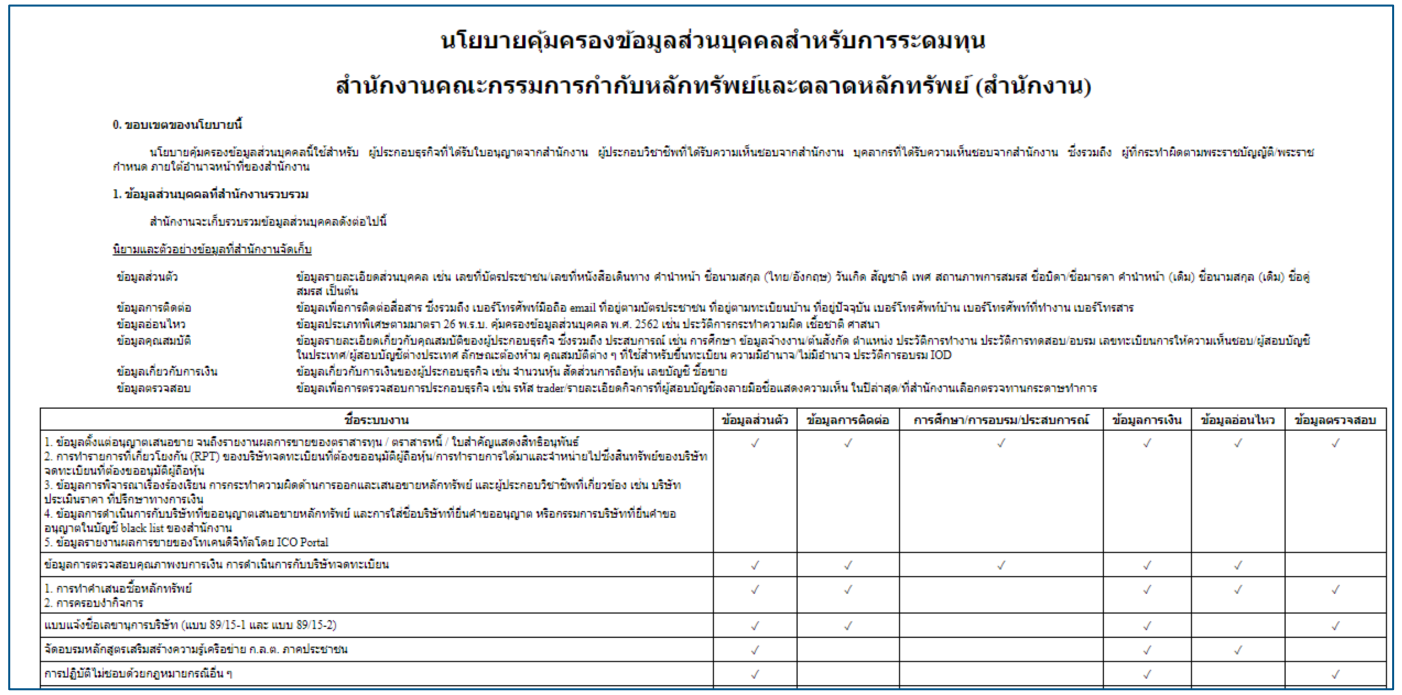


4 จัดทำ Data flow



3 จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน แบ่งตาม subject area (แจ้งเจ้าของข้อมูลทราบ)

https://www.sec.or.th/TH/Pages/PrivacyNotice.aspx



ธรรมาภิบาลข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล ภายในสำนักงาน ก.ล.ต.

- คณะทำงานด้านธรรมาภิบาลข้อมูล
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

นโยบายธรรมาภิบาลข้อมูล

หลักและแนวปฏิบัติตามโยบายธรรมาภิบาลข้อมูล

หลักและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

การบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล (Data Life Cycle)

- การได้มาและการรักษาคุณภาพข้อมูล
- การประมวลผลและการวิเคราะห์ข้อมูล
- การแลกเปลี่ยนและเผยแพร่ข้อมูล
- การเก็บรักษาและทำลายข้อมูล

- ระบุประเภท จัดชั้นความลับ ฐานการประมวลผล และสิทธิการเข้าถึงข้อมูล ม.37
- จัดทำทะเบียนข้อมูลกลางของสำนักงาน ม.39 (แบ่งเป็นข้อมูลส่วนบุคคล และข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล)
- จัดทำ Gap Analysis (ทำเป็น phase เริ่ม Q4/63)
- จัดทำมาตรฐานกำหนดชั้นความลับของข้อมูล
- บันทึกการได้มาของข้อมูล

- ใช้งานตามสิทธิที่ได้รับ
- บันทึกการประมวลผลและวิเคราะห์ข้อมูล

- จัดทำแนวปฏิบัติการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกทั้งในและต่างประเทศ
- บันทึกการแลกเปลี่ยนและเผยแพร่ข้อมูล

- จัดทำมาตรฐานระยะเวลาการจัดเก็บข้อมูล และจัดทำแนวปฏิบัติ
- จัดทำ Alert เมื่อถึงเวลาจัดเก็บข้อมูลถาวร หรือทำลายข้อมูล (กำหนดการเสร็จขึ้นอยู่กับการจัดทำระบบ ECM)
- บันทึกการจัดเก็บข้อมูลและทำลาย

มาตรา 23

การแจ้งการประมวลผลซึ่งทำกันแล้วอย่างกว้างขวางด้วย สิ่งที่เรียกว่า privacy policy

มาตรา 24

ซึ่งในการแจ้งนี้ หลักข้อนึงคือการอธิบายการทำงานได้ด้วยฐานการประมวลข้อมูล

มาตรา 19

กรณีที่ต้องขอความยินยอมก็ต้องมี consent form

มาตรา 37

มาตรการเพื่อความปลอดภัยของข้อมูล หลักๆคืออย่าปล่อยให้ข้อมูล ไม่มี Access Control

มาตรา 39

มีการบันทึกกิจกรรมการประมวลข้อมูลส่วนบุคคลที่ทำกันแล้วอย่างกว้างขวาง ที่เรียกว่า ROP (Record of Processing Activities)

การจัดการเพิ่มเติมตาม PDPA

สถานะ การดำเนินการQ1/64

1.จัดตั้งคณะทำงาน Data Governance Committee และ DPO พร้อมด้วยคณะทำงาน DPO เพื่อให้คำแนะนำและประสานงานกับผู้ที่เกี่ยวข้อง
2.จัดทำมาตรการการรักษาความปลอดภัยรวมถึงการคุ้มครองข้อมูลส่วนบุคคล (เช่น ISO 27001 27701 และ NIST เป็นต้น)
3.จัดทำแบบฟอร์มขอความยินยอม ม.19
4.จัดทำแบบฟอร์ม Privacy Policy และ Privacy Notice ม. 23,24
5.จัดทำบันทึกข้อตกลงกับหน่วยงานภายนอก
- ข้อสัญญามาตรฐานสำหรับการโอนข้อมูล
- ข้อสัญญามาตรฐานสำหรับการประมวลผลข้อมูล
- สัญญารักษาความลับ(NDA)

6.จัดทำมาตรฐานการควบคุมการดำเนินงาน
7.จัดทำแบบฟอร์มและระบบสำหรับการขอใช้สิทธิของเจ้าของข้อมูล
8.จัดทำระบบเก็บ version Privacy policy และส่ง mail แจ้งเจ้าของข้อมูลให้รับทราบ privacy policy ของสำนักงาน
9.จัดทำระบบเก็บ version การขอความยินยอมและการยกเลิกความยินยอม
10.อบรมพนักงานและผู้บริหาร (ผ่านหลักสูตร Online) และประชาสัมพันธ์ผ่าน Infographic
11.จัดทำเกณฑ์ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

การดำเนินการต่อเนื่อง (เริ่ม Q1/64)

1.จัดประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)
2.จัดทำ data flow เพื่อให้ทราบจุดการที่ได้รับข้อมูลเพื่อนำประมวลผลข้อมูล
3.จัดทำ Gap Analysis (ทำเป็น phase เริ่ม Q4/63)
4.จัดทำแนวปฏิบัติการละเมิดข้อมูลหรือข้อมูลรั่วไหล (Data Leakage Prevention, DLP) (ทำเป็น phase)

<u>งานทบทวน ต่อเนื่อง</u>
5.ตรวจสอบนโยบายและแนวปฏิบัติ รวมถึงมาตรฐานต่าง ๆ เช่น ความเหมาะสมและเพียงพอของการรักษาความปลอดภัย
6.ตรวจสอบการดำเนินงานตามนโยบายและแนวปฏิบัติ

การดำเนินการด้าน PDPA ภายนอกสำนักงาน

	เตรียมความพร้อมสำหรับหน่วยงานภายใต้การกำกับ	ความร่วมมือกับหน่วยงานภายนอก (3 Regs) (ก.ล.ต.+ธปท.+คปภ.)
วัตถุประสงค์	เพื่อให้มั่นใจได้ว่าหน่วยงานภายใต้การกำกับสามารถปฏิบัติได้ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างครบถ้วน	เพื่อให้หน่วยงานภายใต้การกำกับสามารถปฏิบัติได้ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยให้สอดคล้องกันทั้งภาคธุรกิจการเงิน
คณะทำงาน	แต่งตั้งคณะทำงาน ประกอบด้วยผู้แทนจากหลายฝ่ายงาน (ตั้งแต่ 22 พ.ค. 63)	แต่งตั้งคณะทำงานร่วมกัน 3Regs (ตั้งแต่ 29 ม.ค. 63) ให้ความเห็น - ข้อเสนอแนะต่อ สคส.
กิจกรรม	☑ ให้คำปรึกษาแก่หน่วยงานฯ เช่น สมาคมบล. บลจ. ☑ ออก Checklist ประเมินความพร้อม+ให้ความรู้(FB Live) ☑ ออกแบบสอบถามเกี่ยวกับ DPO +สนับสนุนการจัดสัมมนาให้ความรู้แก่หน่วยงานฯ ☑ แบบสำรวจความพร้อมในการจัดให้มีธรรมาภิบาลข้อมูลที่ดี และแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ☑ นัดหารือกับ สมาคม บล. บลจ. 24 มี.ค. 64 ☑ ออกแบบสำรวจความพร้อมให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล และธุรกิจอื่นๆ ภายใต้การกำกับ ☑ นัดหารือกับฝ่ายงานที่เกี่ยวข้องและที่ปรึกษา เรื่องการจัดทำกฎเกณฑ์ของสำนักงานให้สอดคล้องกับ PDPA 21 เม.ย. 64	☑ แต่ละหน่วยงานแจ้งความคืบหน้าเกี่ยวกับแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของแต่ละภาคธุรกิจโดยร่วมกัน จัดทำ common issue รวมถึง specific issue และปัญหา อุปสรรคของหน่วยงานภายใต้การกำกับ ☑ ทั้ง 3 หน่วยงานนัดเข้าหารือกับสคส.เพื่อวางแนวทางการออกหลักเกณฑ์ให้สอดคล้องกับกฎหมายลำดับรอง (25 ก.พ. 64) ☑ ทั้ง 3 หน่วยงานนัดหารือร่วมกับสคส. เพื่อแจ้งข้อสังเกตของกฎหมายรองทั้ง 8 ฉบับที่ออกโดย สคส. (31 มี.ค. 64) ☑ แนวทางการประสานงานระหว่างหน่วยงานกำกับดูแลภาคการเงินและสคส. (23 เม.ย. 64)

ยกระดับ Governance & PDPA

แบบสำรวจความพร้อมในการจัดให้มีธรรมาภิบาลข้อมูลที่ดีและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

1. ผู้บริหารและบุคลากร
2. นโยบาย
3. การบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle)
   - 3.1 การได้มาและรักษาคุณภาพข้อมูล
   - 3.2 การใช้และการวิเคราะห์ข้อมูล
   - 3.3 การแลกเปลี่ยนและการเผยแพร่ข้อมูล
   - 3.4 การเก็บรักษาและการทำลายข้อมูล
4. สิทธิของเจ้าของข้อมูล
5. การป้องกันและดำเนินการกรณีข้อมูลรั่วไหล
6. การสื่อสารแนวปฏิบัติ
7. หัวข้ออื่นๆ เช่น ทบทวนแนวปฏิบัติ
8. การสนับสนุนจากสำนักงาน ก.ล.ต.

ความกังวล ความเป็นห่วง
จากการเตรียมความพร้อมของสำนักงาน และหน่วยงานภายใต้การกำกับ

1. รอกฎหมายลำดับรองและแนวปฏิบัติเพื่อให้เกิดความชัดเจนในการปฏิบัติ
2. ปฏิบัติแค่ไหน จึงจะพอ ไม่ผิดกฎหมาย เพราะกฎหมายยังต้องอาศัยการตีความ
3. อยากให้เน้นการสร้างความรู้ความเข้าใจก่อนบังคับใช้กฎหมายเต็มรูปแบบ และยังต้องการการสนับสนุนการให้ความรู้จากส่วนกลาง

Thank You