สำนักงานปลัดกระทรวงพาณิชย์

โครงการจ้างที่ปรึกษาจัดทำการคุ้มครองข้อมูลส่วนบุคคล ของสำนักงานปลัดกระทรวงพาณิชย์ให้รองรับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

Project Kick-off

6 ธันวาคม 2565

หัวข้อนำเสนอ

1. ภาพรวมงานโครงการ
2. โครงสร้างบุคลากรในโครงการ
3. ขอบเขตการดำเนินงาน (Scope of Work)
4. สิ่งส่งมอบงานโครงการ
5. กรอบแนวคิด เครื่องมือ มาตรฐานและแนวปฏิบัติอ้างอิง
6. เอกสาร PDPA เทียบกับกฎหมายแต่ละมาตรา
7. แผนดำเนินงานโครงการ (Project Plan)
8. ข้อเสนอแนะการจัดตั้งโครงสร้างการกำกับดูแลฯ
9. ถาม-ตอบ

1. ภาพรวมงานโครงการ

ภาพรวมงานโครงการ (Project: Executive Summary)

Project Information - Executive Summary	
ชื่อโครงการ	▪ โครงการจ้างที่ปรึกษาจัดทำการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงพาณิชย์ให้รองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
วัตถุประสงค์หลัก	▪ เพื่อจัดทำมาตรการการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงพาณิชย์ ให้รองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
ผลลัพธ์ (Outcome)	▪ มาตรการคุ้มครองข้อมูลส่วนบุคคลและเอกสารต้นแบบที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำหรับ สำนักงานปลัดกระทรวงพาณิชย์
ระยะเวลาโครงการ	▪ ระยะเวลาโครงการ : 240 วัน นับถัดจากวันลงนามในสัญญา

General Data Protection Regulation (GDPR)

Fines Database

Total Number of GDPR Fines
1216

Total Amount of GDPR Fines
€2,042,417,507

Largest Fine
€746,000,000
Amazon Europe Core S.a.r.l. on July 22 , 2021 - Luxembourg

Smallest Fine
€28
Unknown on November 18 , 2020 - Hungary

Most Recent GDPR Fines

*Only includes finalised cases

DATE	ORG	FINE
11/21/2022	ING BANK NV Amsterdam Sucursala București	€20,000
11/21/2022	Private individual	€300
11/18/2022	Homeowners Association Bld. Pipera 1-2E	€300
11/16/2022	Raiffeisen Bank SA	€28,000
11/15/2022	BANKINTER, S.A.	€80,000

TOP 5 BIGGEST GDPR FINES

*Only includes final & binding fines

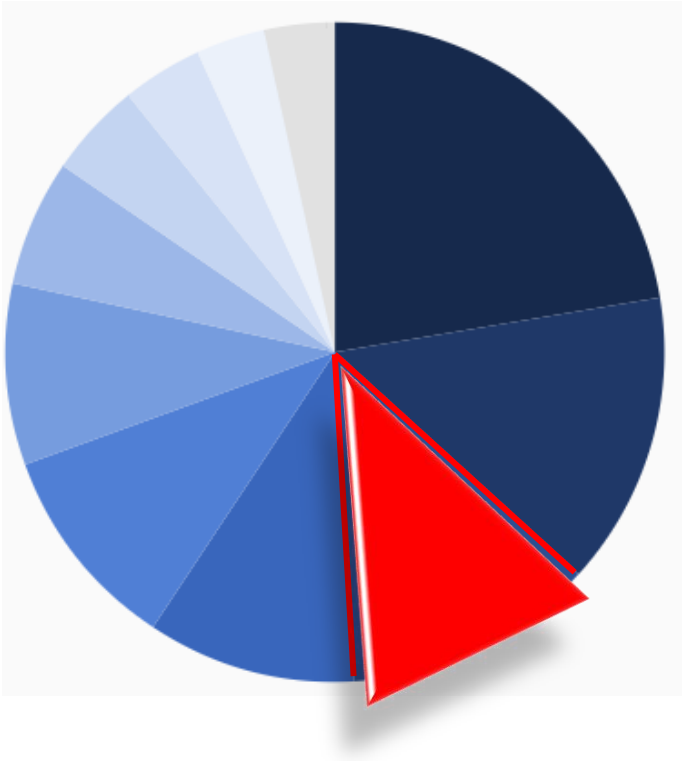
Amazon Europe Core S.a.r.l.	€746,000,000
Meta Platforms, Inc. (Facebook)	€405,000,000
WhatsApp	€225,000,000
Google LLC	€90,000,000
Facebook Ireland Ltd.	€60,000,000

ETid-1507	SPAIN	2022-11-29	3,000	Company	Art. 6 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
ETid-1506	FRANCE	2022-11-24	600,000	ÉLECTRICITÉ DE FRANCE	Art. 7 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. L. 34-5 CPCE	Insufficient fulfilment of data subjects rights
ETid-1505	ITALY	2022-11-10	500,000	Vodafone Italia S.p.A.	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 130 (1), (2), (3) Codice della privacy	Non-compliance with general data processing principles
ETid-1504	SPAIN	2022-11-29	1,000	Private individual	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
ETid-1503	ROMANIA	2022-11-25	3,000	OTP LEASING ROMANIA IFN SA	Art. 25 (1) GDPR, Art. 32 (1) b) GDPR, Art. 32 (2) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-1502	IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-1501	ROMANIA	2022-11-24	1,000	Medicover S.R.L.	Art. 32 (1) b) GDPR, Art. 32 (2) GDPR, Art. 32 (4) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-1500	ROMANIA	2022-11-21	20,000	ING Bank NV Amsterdam Sucursala București	Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-1499	SPAIN	2022-11-21	300	Private individual	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
ETid-1498	PORTUGAL	2022-11-02	180,000	Setúbal municipality	Art. 5 (1) e), f) GDPR, Art. 13 (1), (2) GDPR, Art. 37 (1), (7) GDPR	Non-compliance with general data processing principles

Source: https://www.privacyaffairs.com/gdpr-fines/ & https://www.enforcementtracker.com

General Data Protection Regulation (GDPR)

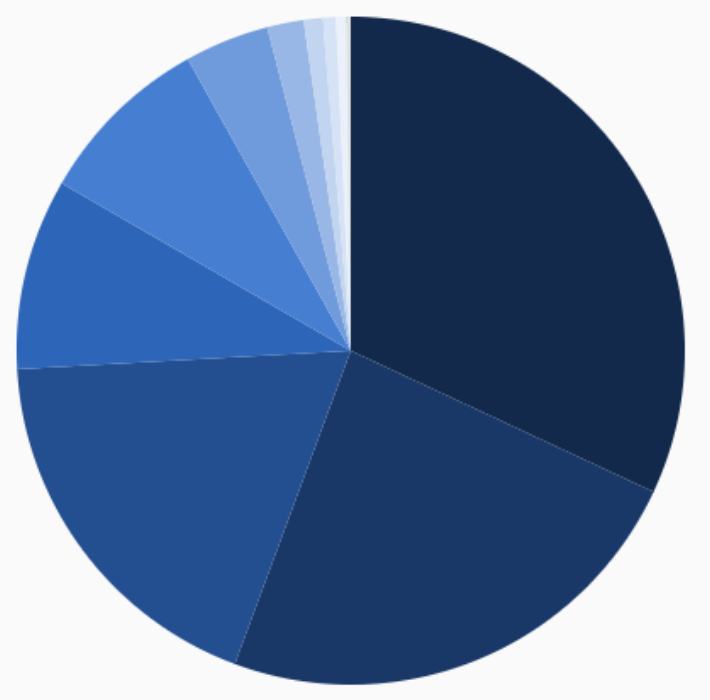
by Sectors



Sector	Number of Fines
Industry and Commerce	**317** (with total € 854,287,397)
Media, Telecoms and Broadcasting	**204** (with total € 1,030,557,541)
Public Sector and Education	**175** (with total € 19,524,763)
Finance, Insurance and Consulting	**145** (with total € 34,400,108)
Individuals and Private Associations	**144** (with total € 1,531,116)
Health Care	**126** (with total € 14,951,009)
Employment	**88** (with total € 47,945,677)
Transportation and Energy	**66** (with total € 84,854,214)
Not assigned	**56** (with total € 750,308)
Accomodation and Hospitalty	**48** (with total € 22,109,657)
Real Estate	**43** (with total € 2,577,570)
Unknown	**6** (with total € 48,040)

General Data Protection Regulation (GDPR)

by Type of violation



Violation	Number of Fines
Insufficient legal basis for data processing	**453** (with total € 450,410,237)
Non-compliance with general data processing principles	**336** (with total € 1,253,258,499)
Insufficient technical and organisational measures to ensure information security	**262** (with total € 110,713,219)
Insufficient fulfilment of data subjects rights	**131** (with total € 49,104,070)
Insufficient fulfilment of information obligations	**121** (with total € 237,002,475)
Insufficient cooperation with supervisory authority	**58** (with total € 309,029)
Insufficient fulfilment of data breach notification obligations	**25** (with total € 1,497,161)
Insufficient involvement of data protection officer	**13** (with total € 875,600)
Insufficient data processing agreement	**9** (with total € 1,048,610)
Unknown	**7** (with total € 9,229,500)
Insuffcient fulfilment of data subject rights	**3** (with total € 89,000)

1) British Airways

กรณีสายการบินบริติช แอร์เวย์ในเดือนมิถุนายน 2561 ที่เว็บไซต์ของสายการบินมีการ**เปลี่ยนเส้นทางไปสู่หน้าเพจหลอกขโมยข้อมูลของมิจฉาชีพ ทำให้ข้อมูลของลูกค้าที่ซื้อตั๋วเครื่องบินผ่านทางเว็บไซต์ราว ๆ 500,000 รายตกไปอยู่ในมือแฮ็คเกอร์**โดยมีทั้งข้อมูลล็อคอิน ข้อมูลการเดินทาง ชื่อ ที่อยู่ หมายเลขบัตรเครดิต ข้อมูลวันหมดอายุ เลข CVV 3 หลัก ฯลฯ บริติช แอร์เวย์โดนสำนักงานคณะกรรมาธิการด้านข้อมูล (ICO) สหราชอาณาจักรสั่งลงโทษ**ปรับเป็นจำนวน 204.6 ล้านยูโร (ประมาณ 8,184 ล้านบาท)**

2) Marriott International Hotel

เครือโรงแรมแมริออตต์ของสหรัฐ ถูกสำนักงาน ICO สหราชอาณาจักร **สั่งปรับ 110.3 ล้านยูโร (4,412 ล้านบาท) จากเหตุการณ์ที่แฮกเกอร์เปิดเผยข้อมูลส่วนบุคคลที่เซนซิทีฟอย่างหมายเลขบัตรเครดิต หมายเลขพาสปอร์ต วันเดือนปีเกิดลูกค้ากว่า 300 ล้านราย**ซึ่งกว่า 30 ล้านรายเป็นประชากรสหภาพยุโรป

3) Google

แม้กรณีของยักษ์ใหญ่แห่งวงการดิจิทัล Google จะไม่ใช่การถูกล่วงละเมิดข้อมูล แต่ Google ก็ถูกทางการฝรั่งเศส**สั่งปรับเงินจำนวน 50 ล้านยูโร (ประมาณ 200 ล้านบาท)** เพราะ**ผู้ใช้งานไม่สามารถเข้าถึงรายงานประมวลผลข้อมูลผู้บริโภค (consumer data processing statement)** ได้โดยง่าย และภาษาที่ใช้อธิบายก็กำกวมไม่ชัดเจน ยิ่งไปกว่านั้น Google ยังมีความผิดที่**ไม่ขอความยินยอมจากผู้บริโภคในการนำขอข้อมูลมาใช้ทำแคมเปญโฆษณาแบบ targeting** ซึ่งผิดกฎหมาย GDPR

4) Austrian Post

เหตุการณ์นี้เกิดในช่วงต้นปี 2562 ที่ Austrian Post **หน่วยงานไปรษณีย์ของออสเตรียถูกหน่วยงานป้องกันข้อมูลแห่งชาติสั่งปรับ 18.5 ล้านยูโร (ประมาณ 740 ล้านบาท) โทษฐานขายข้อมูลผู้บริโภคโดยมิชอบ**ซึ่งเป็นการละเมิดข้อบังคับ GDPR ทั้งนี้จากการตรวจสอบพบว่า Austrian Post ได้ทำการตรวจดูข้อมูลผู้บริโภคว่าใครมีแนวโน้มลงคะแนนเสียงที่พวกเขาสนับสนุนอยู่และขายข้อมูลเหล่านั้น

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

ความรับผิดและบทลงโทษ:

1. **ความรับผิดทางแพ่ง => เจ้าของข้อมูลฟ้องศาล => ชดใช้ค่าสินไหมทดแทน**
2. **โทษทางอาญา => เจ้าของข้อมูลฟ้องศาล => จำคุก หรือปรับเงิน หรือทั้งจำทั้งปรับ**
3. **โทษทางปกครอง => สำนักงานคุ้มครองข้อมูลส่วนบุคคลดำเนินการ => ต้องระวางโทษปรับทางปกครองตั้งแต่ไม่เกิน 1 ล้านบาท ถึง 5 ล้านบาท**

หมวด ๖ ความรับผิดทางแพ่ง (มาตรา ๗๗ – มาตรา ๗๘):

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆเกี่ยวกับข้อมูลส่วนบุคคลอันเป็น การฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล เว้นแต่ ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคาสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย => **ค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น**

สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้เป็นอันขาดอายุความเมื่อพ้นสามปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือเมื่อพ้นสิบปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

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

หมวด ๗ บทกำหนดโทษ ส่วนที่ ๑ โทษอาญา (มาตรา ๗๙ – มาตรา ๘๑) => จำคุก หรือปรับเงิน หรือทั้งจำทั้งปรับ

มาตรา ๗๙ ใช้ หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอม หรือไม่เป็นไปตามการประมวลผลตามฐานกฎหมายอื่น ๆ ที่ได้รับการยกเว้นตามมาตรา 24 และ 26 (มาตรา ๒๗ วรรค ๑) / ใช้ หรือเปิดเผย (ประมวลผลข้อมูล) ที่อยู่นอกเหนือจากวัตถุประสงค์ที่ได้แจ้ง ๆ ไว้ (มาตรา ๒๗ วรรค ๒) / ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา (มาตรา ๒๘)

=> จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้าน หรือทั้งจำทั้งปรับ

มาตรา ๘๐ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนาไปเปิดเผยแก่ผู้อื่น

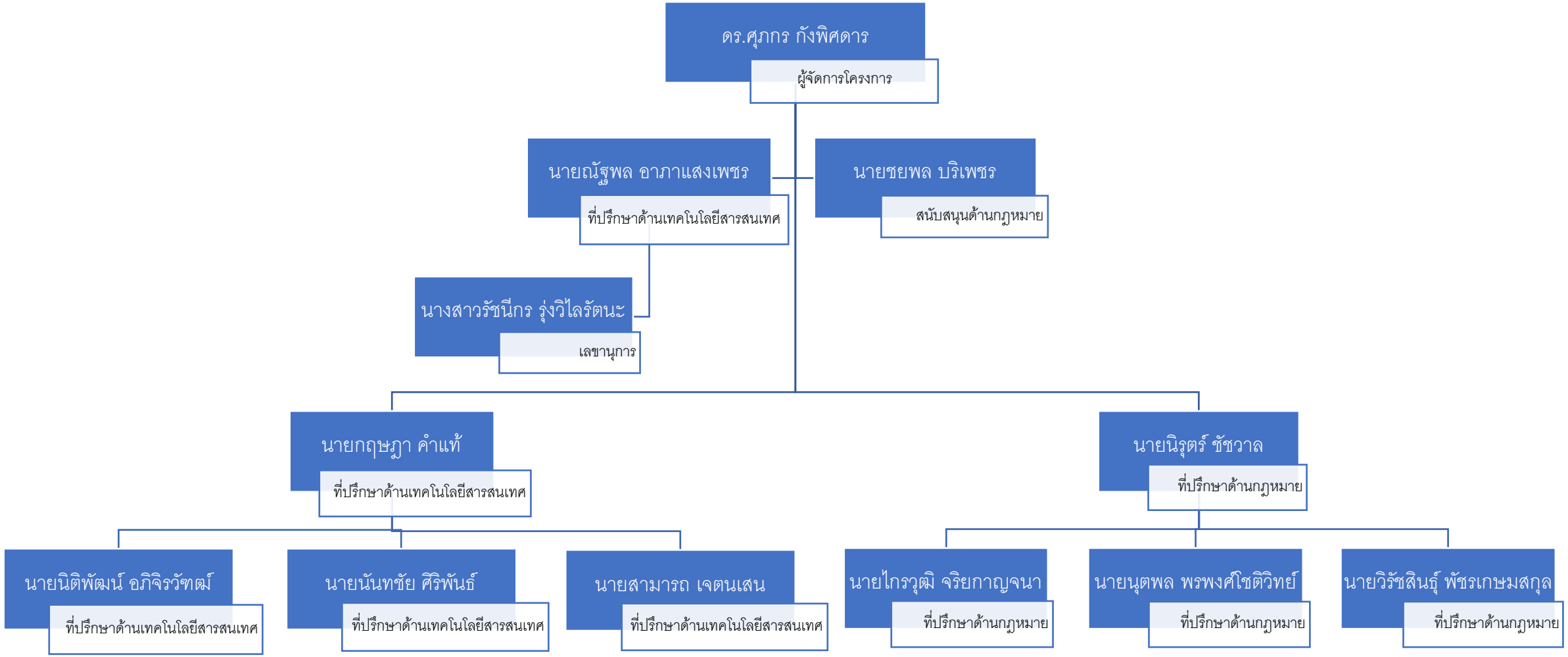
=> จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสน หรือทั้งจำทั้งปรับ

มาตรา ๘๑ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใด ซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด **ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย**

ส่วนที่ ๒ โทษทางปกครอง (มาตรา ๘๒ – มาตรา ๙๐) => ต้องระวางโทษปรับทางปกครองตั้งแต่ไม่เกินหนึ่งล้านบาท ถึงห้าล้านบาท

2. โครงสร้างบุคลากรในโครงการ

โครงสร้างบุคลากรในโครงการ



3. ขอบเขตการดำเนินงาน (Scope of Work)

ภาพรวมขอบเขตการดำเนินงาน (Scope of Work)

ดำเนินการให้คำปรึกษาโดยนำหลักการหรือข้อกำหนดตามมาตรฐาน ISO/IEC 27701 และมาตรฐานหรือแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มาประยุกต์ใช้กับสำนักงานปลัดกระทรวงพาณิชย์ เพื่อปรับปรุงมาตรการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยขอบเขตงานจะครอบคลุมการดำเนินในสำนักงานปลัดกระทรวงพาณิชย์

2. ศึกษา/วิเคราะห์ภารกิจของ สป.พณ. และให้คำปรึกษา ให้คำแนะนำในการจัดทำเอกสารให้สอดคล้องและถูกต้องตามกฎหมาย

จัดทำการศึกษา วิเคราะห์ และให้คำแนะนำในการจัดทำเอกสารให้สอดคล้องและถูกต้องตามกฎหมาย ในการดำเนินการเพื่อให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ สำหรับด้านธรรมาภิบาลข้อมูลภาครัฐ

ตามหัวข้อ TOR 4.1 การดำเนินโครงการ

จัดทำแผนการดำเนินงานโครงการ (Project Plan) พร้อมแผนปฏิบัติการ (Action Plan) ที่แสดงกำหนดระยะเวลาการดำเนินโครงการ (Timeline) ที่ชัดเจน เพื่อพิจารณาเห็นชอบ ภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา โดยต้องประกอบด้วยรายละเอียดอย่างน้อย ได้แก่ กรอบแนวคิด วิธีการ ขั้นตอน แผนการดำเนินโครงการฯ ที่ระบุกิจกรรม ระยะเวลาในแต่ละกิจกรรม บุคลากรที่รับผิดชอบ งวดการส่งมอบงาน และแสดงผลลัพธ์ของการดำเนินงานรายกิจกรรม ให้แก่ สป.พณ. โดยขอบเขตของกิจกรรมที่ให้คำปรึกษาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

4.1.1 ส่วนกลาง ประกอบด้วย

1) กองกลาง
2) กองตรวจราชการ
3) กองบริหารการคลัง
4) กองบริหารการพาณิชย์ภูมิภาค
5) กองบริหารทรัพยากรบุคคล
6) กองยุทธศาสตร์และแผนงาน
7) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
8) สถาบันกรมพระจันทบุรีนฤนาถ
9) กลุ่มกฎหมาย
10) กลุ่มตรวจสอบภายใน
11) กลุ่มพัฒนาระบบบริหาร
12) ศูนย์ปฏิบัติการต่อต้านการทุจริต
13) สำนักงานรัฐมนตรี

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.1.2 สำนักงานในส่วนภูมิภาค ประกอบด้วย สำนักงานพาณิชย์จังหวัดทั้งหมด

4.1.3 สำนักงานในต่างประเทศ ประกอบด้วย

1) สำนักงานพาณิชย์ในต่างประเทศ ณ กรุงวอชิงตัน ดี ซี

2) สำนักงานพาณิชย์ในต่างประเทศ ณ กรุงบรัสเซลส์

3) สำนักงานพาณิชย์ในต่างประเทศ ณ กรุงปักกิ่ง

4) คณะผู้แทนถาวรไทยประจำองค์การการค้าโลกและองค์การทรัพย์สินทางปัญญาโลก (เจนีวา)

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตามหัวข้อ TOR 4.2 ศึกษา/วิเคราะห์ภารกิจของ สป.พณ. และให้คำปรึกษา ให้คำแนะนำในการจัดทำเอกสารให้สอดคล้องและถูกต้องตามกฎหมาย ในการดำเนินการเพื่อให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ สำหรับด้าน
ธรรมาภิบาลข้อมูลภาครัฐ โดยมีรายละเอียดครอบคลุมในด้านต่าง ๆ อย่างน้อยดังต่อไปนี้

4.2.1 การศึกษา สำรวจ ประเมินความพร้อมด้านธรรมาภิบาลข้อมูลภาครัฐ ของสำนักงานปลัดกระทรวงพาณิชย์ พร้อมให้คำแนะนำ ตลอดจนแนวทางต่าง ๆ ให้สอดคล้องกับธรรมาภิบาสข้อมูลภาครัฐ

4.2.2 การวิเคราะห์ข้อมูลของสำนักงานปลัดกระทรวงพาณิชย์ให้เป็นไปตามแนวทางที่ภาครัฐกำหนด เช่น แนวทางการบริหารจัดการข้อมูล คุณภาพข้อมูล ความสามารถเชื่อมโยงแลกเปลี่ยน และความสอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ

4.2.3 การทบทวน/ปรับปรุงให้ข้อเสนอแนะ ด้านนโยบาย กฎ ระเบียบ และเอกสารที่เกี่ยวข้องกับธรรมาภิบาสข้อมูลภาครัฐ ของสำนักงานปลัดกระทรวงพาณิชย์ ตามที่รัฐกำหนด

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตามหัวข้อ TOR 4.3 ศึกษาวิเคราะห์ภารกิจของ สป.พณ. และจัดทำเอกสารให้สอดคล้องและถูกต้องตามกฎหมายในการดำเนินการเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยมีรายละเอียดดังต่อไปนี้

4.3.1 เสนอแนะ ให้คำปรึกษา ในการกำหนดหน้าที่และความรับผิดชอบในการดำเนินการต่าง ๆ ของคณะกรรมการ คณะทำงาน และบุคลากร ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล รวมทั้งจัดทำร่างประกาศข้อกำหนด คำสั่งแต่งตั้งคณะกรรมการ คณะทำงาน และเจ้าหน้าที่ดังกล่าว พร้อมทั้งให้ข้อเสนอแนะให้คำปรึกษาที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล แก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) คณะกรรมการ คณะทำงาน และเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อให้ สป.พณ. ปฏิบัติได้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

4.3.2 ประเมินสถานะกระบวนงานข้อมูลส่วนบุคคล (Gap Analysis Assessment) ของ สป.พณ. โดยประเมินช่องว่างกิจกรรมที่เกี่ยวข้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓ ให้ข้อเสนอแนะ และกำหนดระดับความพร้อมการกำกับดูแลติดตามการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องตามที่กฎหมายกำหนด พร้อมทั้งให้ความรู้กับคณะทำงานพร้อมทั้งให้ความรู้กับคณะทำงาน

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3.3 การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA) ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

4.3.3.1 จัดอบรมให้ความรู้ หรือการประชุมเชิงปฏิบัติการ (Workshop) (ระยะเวลารวมไม่น้อยกว่า ๗๘ ชั่วโมง และผู้เข้าร่วมรวมไม่น้อยกว่า ๑๓๐ คน) ให้แก่เจ้าหน้าที่ที่เกี่ยวข้อง เพื่อเตรียมความพร้อมการดำเนินการให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยครอบคลุมประเด็นอย่างน้อย
ดังนี้ ความตระหนักรู้และสำนึกรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล หน้าที่ความรับผิดชอบของหน่วยงาน การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ผลกระทบที่เกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล แนวทางการตรวจสอบระบบคุ้มครองข้อมูลส่วนบุคคล

4.3.3.2 สร้างชุดคำถาม (Questionnaire) และดำเนินการเก็บรวบรวมข้อมูลจากเจ้าหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานต่าง ๆ ในองค์กร พร้อมประเมินความเสี่ยงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยจัดทำบันทึกข้อมูลผ่านชุดคำถามให้กับหน่วยงานต่าง ๆ ในสังกัด สป.พณ. ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล พร้อมจัดทำ Data Inventory ของ สป.พณ.

4.3.3.3 สอบถามเจ้าหน้าโดยสัมภาษณ์กลุ่ม (Focus Group) (ระยะเวลารวมไม่น้อยกว่า ๗๘ ชั่วโมง และผู้เข้าร่วมรวมไม่น้อยกว่า ๑๓๐ คน) เพื่อระบุรายละเอียดเพิ่มเติมเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอ่อนไหว การเก็บรวบรวม ใช้ และเปิดเผยต่อบุคคลหรือหน่วยงานภายนอก รวมถึงบทบาทขององค์กร และฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูล โดยใช้วิธีสัมภาษณ์ผ่านสื่ออิเล็กทรอนิกส์หรือ ณ ที่ทำการของ สป.พณ. ตามที่ณะกรรมการตรวจรับพัสดุเห็นสมควร รวมทั้งบันทึกภาพและ/หรือเสียงการจัดกิจกรรมในรูปแบบวิดีโอ พร้อมส่งมอบไฟล์อิเล็กทรอนิกส์

4.3.3.4 จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) เพื่อตรวจสอบกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งองค์กรกำลังดำเนินการอยู่ โดยเริ่มตั้งแต่วิธีการเก็บ การจัดเก็บ การถ่ายโอนข้อมูล การลบข้อมูล รวมไปถึงมาตรการด้านนโยบายและด้านเทคนิค เพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยเสนอแนะระบบบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ช่วยเหลือในการดำเนินงาน

4.3.3.5 ให้คำแนะนำแก่พนักงาน เจ้าหน้าที่ ผู้รับผิดชอบกิจกรรม และสอบถามข้อมูลเพิ่มเติมเพื่อแก้ไขให้บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) สมบูรณ์เป็นปัจจุบัน

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3.3.6 จัดทำรายงานบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA Report) เพื่อสร้างประวัติการจัดทำบันทึกรายการกิจกรรมฉบับปัจจุบัน โดยมีรายละเอียดสอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างน้อยดังนี้

1) สรุปจำนวนกิจกรรมตามสำนักงาน/กอง/ศูนย์/สถาบัน/กลุ่ม

2) แผนภาพแสดงการไหลของข้อมูลในแต่ละสำนักงาน/กอง/ศูนย์/สถาบัน/กลุ่ม (Data Flow / Data Mapping)

3) ประเภทของข้อมูลส่วนบุคคลที่องค์กรใช้ประมวลผล และประเภทเจ้าของข้อมูลส่วนบุคคล

4) สถานที่จัดเก็บข้อมูล

5) ระยะเวลาการจัดเก็บข้อมูล

6) การถ่ายโอนข้อมูล

7) ประเมินภาพรวมและข้อเสนอแนะความเสี่ยง

8) การดำเนินการให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมาย

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3.4 ศึกษา/วิเคราะห์ภารกิจของ สป.พณ. และจัดทำเอกสารให้สอดคล้องและถูกต้องตามกฎหมายในการจัดทำเอกสารกฎหมายคุ้มครองข้อมูลส่วนบุคคล

4.3.4.1 ร่างและจัดทำแบบนโยบายและเอกสารทางกฎหมายที่จำเป็นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยต้องมีเนื้อหาครอบคลุมหลักการที่สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ครอบคลุมประเด็นต่าง ๆ อย่างน้อย ดังนี้ การรวบรวมและจัดเก็บข้อมูลเท่าที่จำเป็น การใช้และเปิดเผยข้อมูลอย่างจำกัด การรักษาความมั่นคงปลอดภัยข้อมูล การกำหนดวัตถุประสงค์ให้ชัดเจน การรักษาคุณภาพของข้อมูล ความมีส่วนร่วมของเจ้าของข้อมูล การเปิดเผยข้อมูลให้สอดคล้องกับกฎหมาย ความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

1) นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

2) หนังสือให้ความยินยอมฉบับมาตรฐาน ที่จำเป็นตามรูปแบบองค์กรและกิจกรรม (Consent Form) รวมถึงขั้นตอนปฏิบัติในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure)

3) ประกาศความเป็นส่วนตัว (Privacy Notice)

4) ข้อตกลงการประมวลผลข้อมูลฉบับมาตรฐาน ที่จำเป็นตามรูปแบบองค์กรและกิจกรรม (Data Processing Agreement)

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5) กระบวนการจัดการปัญหาเมื่อเกิดข้อร้องเรียน และ/หรือ การละเมิดการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach Procedure)

6) เอกสารบันทึกการแจ้งเหตุละเมิด

7) ขั้นตอนหรือแนวปฏิบัติเพื่อรองรับการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) สำหรับเจ้าหน้าที่และเจ้าของข้อมูลส่วนบุคคล เช่น การแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล และคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

8) นโยบาย แนวปฏิบัติและเอกสารอื่น ๆ ของหน่วยงาน ที่จำเป็นอย่างน้อย ดังนี้

(๑) จัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement)

(๒) นโยบายคุกกี้ (Cookies Policy)

(๓) เอกสารที่เกี่ยวข้องกับกระบวนการบริหารงานบุคคล

(๔) แนวทางการกำกับและติดตามผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล

(๕) แนวทางการตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล

(๖) อื่น ๆ (หากมี) โดยเนื้อหาจะต้องสอดคล้องตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนด พร้อมทั้งให้คำแนะนำการดำเนินงานในขั้นตอนต่าง ๆ เพื่อให้คำสั่ง/นโยบายข้างต้นถูกต้องตามกระบวนการของกฎหมาย ตามพระราชบัญญัติฯ เช่น การส่งนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาก่อนการประกาศใช้ (ถ้ามีข้อกำหนด)

4.3.4.2 จัดทำหรือแก้ไขปรับปรุงแบบฟอร์มเอกสารทางกฎหมายให้สอดคล้องกับกิจกรรมขององค์กร

4.3.4.3 ตรวจสอบและให้คำแนะนำเกี่ยวกับเอกสารทางกฎหมายที่จำเป็นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

4.3.5 การประเมินความเสี่ยงพื้นฐานตามกฎหมาย

4.3.5.1 ทบทวนตรวจสอบบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) และจัดทำรายงานบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA Report) ฉบับล่าสุดเพื่อให้ข้อมูลเป็นปัจจุบัน ซึ่งมีรายละเอียดเพิ่มเติม ดังนี้

1) ภาพรวมและจำนวนการแก้ไขบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA)

2) รายการปรับปรุงแก้ไขบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.3.5.2 จัดทำรายงานการวิเคราะห์ช่องว่างและข้อบกพร่องพื้นฐาน (Basic Gap Analysis Report) เพื่อวิเคราะห์ช่องว่างและข้อบกพร่องจากบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ฉบับล่าสุด เปรียบเทียบกับข้อกำหนดหรือความต้องการในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งประเมินจากกิจกรรมการประมวลผล ประเภทและความเสี่ยงของช่องว่างพร้อมจัดทำแนวทางการแก้ไขช่องว่างทางกฎหมาย

1) ดำเนินการประเมินความเสี่ยงด้านความเป็นส่วนตัว (Privacy Risk)

2) ดำเนินการประเมินความเสี่ยงด้านความปลอดภัย (Security Risk)

ตามหัวข้อ TOR 4.4 จัดกิจกรรมให้ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงานและเสริมสร้างความรู้ความเข้าใจอันดี ให้มีความตระหนักและรู้เท่าทันในมิติต่าง ๆ สร้างความเข้าใจในแนวปฏิบัติที่กำหนดขึ้น พร้อมเสนอรายละเอียดต่อคณะกรรมการฯ รวมทั้งบันทึกภาพและเสียงการจัดกิจกรรมในรูปแบบวิดีโอ พร้อมส่งมอบไฟล์วิดีโอ (ผู้เข้าร่วมไม่น้อยกว่า ๑๐๐ คน)

จัดทำการคุ้มครองข้อมูลส่วนบุคคลให้รองรับกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตามหัวข้อ TOR ๖. เงื่อนไขทั่วไป

๖.๑ ส่งแผนปฏิบัติงานของที่ปรึกษาและรายชื่อทีมงาน ภายใน ๑๕ วันนับถัดจากวันลงนามในสัญญาและคณะกรรมการฯ เห็นชอบแผนฯ ก่อนดำเนินการ

๖.๒ จัดประชุมเปิดโครงการ (Kick Off) ภายใน ๑๕ วันนับถัดจากวันลงนามในสัญญา พร้อมเสนอรายละเอียดต่อคณะกรรมการฯ รวมทั้งบันทึกภาพและเสียงการจัดกิจกรรมในรูปแบบวิดีโอ พร้อมส่งมอบไฟล์วิดีโอ (ผู้เข้าร่วมไม่น้อยกว่า ๓๐ คน)

๖.๓ รายงานความก้าวหน้าการดำเนินงาน (Progress Report) ประจำเดือนโดยรวบรวมส่งตามงวดงาน

๖.๔ ผลงานภายใต้การดำเนินงานทั้งหมดถือเป็นลิขสิทธิ์ของกระทรวงพาณิชย์

๖.๕ ที่ปรึกษาเป็นผู้รับผิดขอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นในโครงการ

๖.๖ การส่งมอบงานในแต่ละงวดให้จัดส่งในรูปแบบเอกสารอย่างน้อยจำนวน ๘ ชุด (ต้นฉบับ ๑ ชุดและสำเนา ๗ ชุด) พร้อมไฟล์เอกสารในรูปแบบอิเล็กทรอนิกส์ที่สามารถแก้ไขได้ เช่น ,docx, xlsx,.pptx

และเอกสารในรูปแบบ .pdf พร้อมบันทึกลงในสื่อบันทึกข้อมูล Flash Drive

๖.๗ กรณีเกิดเหตุสุดวิสัยหรือตามประกาศของภาครัฐไม่สามารถดำเนินการในรูปแบบปกติได้ ที่ปรึกษา

สามารถดำเนินการโดยผ่านสื่ออิเล็กทรอนิกส์ได้ ทั้งนี้ต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา และหากมีค่าใช้จ่ายส่วนต่างที่เกิดขึ้นจากการดำเนินการดังกล่าว ที่ปรึกษาจะต้องแจกแจง รายละเอียดในการเพิ่มลดให้เหมาะสมกับงบประมาณที่ได้รับ และปรับกิจกรรมทดแทนตามจำนวนสัดส่วนดังกล่าว

4. สิ่งส่งมอบงานโครงการ

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

1

งวดที่ 1
ภายใน 30 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 1 : กำหนดส่งมอบ 22 ธันวาคม 2565 (กำหนดส่งมอบก่อน 7 วัน : 15 ธันวาคม 2565)

(1) แผนการดำเนินงานโครงการ (Project Plan) พร้อมแผนปฏิบัติการ (Action Plan) (TOR 4.1)

(2) รายงานความก้าวหน้าการดำเนินงาน (Progress Report) ประจำเดือน (TOR 6.3)

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

2

งวดที่ 2
ภายใน 90 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 1 : กำหนดส่งมอบ 21 กุมภาพันธ์ 2565 (กำหนดส่งมอบก่อน 7 วัน : 14 กุมภาพันธ์ 2565)

(1) เอกสารการศึกษา สำรวจ การวิเคราะห์ประเมินความพร้อมด้านธรรมาภิบาลข้อมูลภาครัฐ และการทบทวน/ปรับปรุงให้ข้อเสนอแนะด้านนโยบาย กฎ ระเบียบ ของ สป.พณ ตามที่รัฐกำหนด (TOR 4.2)

(2) (ร่าง) เอกสาร DPO Role & Responsibility และ (ร่าง) ประกาศแต่งตั้ง ประกาศ กำหนด คณะกรรมการ คณะทำงาน และเจ้าหน้าที่ฝึกอบรมให้ความรู้ทางวิชาการด้านเทคโนโลยีสารสนเทศแก่บุคลากร (TOR 4.3.1)

(3) เอกสารประเมินสถานะกระบวนงานข้อมูลส่วนบุคคล (Gap Analysis Assessment) (TOR 4.3.2)

(4) บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA) (TOR 4.3.3)

(5) อบรมสร้างความตระหนักแก่ทีมงาน (Working Team) หรือเจ้าหน้าที่ที่เกี่ยวข้อง และการประชุมเชิงปฏิบัติการ (Workshop) ให้แก่เจ้าหน้าที่ที่เกี่ยวข้องเพื่อเตรียมความพร้อม(TOR 4.3.3.1)

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

2

งวดที่ 2
ภายใน 90 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 2: กำหนดส่งมอบ 21 กุมภาพันธ์ 2565 (กำหนดส่งมอบก่อน 7 วัน : 14 กุมภาพันธ์ 2565)

(6) สร้างชุดคำถาม (Questionnaire) พร้อมประเมินความเสี่ยงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (TOR 4.3.3.2)

(7) จัดกิจกรรมสัมภาษณ์กลุ่ม (Focus Group) (TOR 4.3.3.3)

(8) รายงานบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA Report) (TOR 4.3.3.6)

(9) รายงานความก้าวหน้าการดำเนินงาน (Progress Report) ประจำเดือน (TOR 6.3)

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

3

งวดที่ 3
ภายใน 240 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 3 : กำหนดส่งมอบ 21 กรกฎาคม 2565 (กำหนดส่งมอบก่อน 7 วัน : 14กรกฎาคม 2565)

(1) รายงานความก้าวหน้าการดำเนินงาน (Progress Report) ประจำเดือน (TOR 6.3)

(2) นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) (TOR 4.3.4.1(1))

(3) หนังสือให้ความยินยอมฉบับมาตรฐาน (Consent Form) (TOR 4.3.4.1(2))

(4) ขั้นตอนปฏิบัติในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure) (TOR 4.3.4.1(2))

(5) ประกาศความเป็นส่วนตัว (Privacy Notice) (TOR 4.3.4.1(3))

(6) ข้อตกลงการประมวลผลข้อมูลฉบับมาตรฐาน ที่จำเป็นตามรูปแบบองค์กรและกิจกรรม (Data Processing Agreement) (TOR 4.3.4.1(4))

(7) กระบวนการจัดการปัญหาเมื่อเกิดข้อร้องเรียน และ/หรือ การละเมิดการรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach Procedure) (TOR 4.3.4.1(5))

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

3

งวดที่ 3
ภายใน 240 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 3 : กำหนดส่งมอบ 21 กรกฎาคม 2565 (กำหนดส่งมอบก่อน 7 วัน : 14กรกฎาคม 2565)

(8) เอกสารบันทึกการแจ้งเหตุละเมิด (TOR 4.3.4.1(6))

(9) ขั้นตอนหรือแนวปฏิบัติเพื่อรองรับการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management) สำหรับเจ้าหน้าที่และเจ้าของข้อมูลส่วนบุคคล (TOR 4.3.4.1(7))

(10) ข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement) (TOR 4.3.4.1(8(1)))

(11) นโยบายคุกกี้ (Cookies Policy) (TOR 4.3.4.1(8(2)))

(12) เอกสารที่เกี่ยวข้องกับกระบวนการบริหารงานบุคคล (TOR 4.3.4.1(8(3)))

(13) แนวทางการกำกับและติดตามผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (TOR 4.3.4.1(8(4)))

(14) แนวทางการตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (TOR 4.3.4.1(8(5)))

(15) จัดทำหรือแก้ไขปรับปรุงแบบฟอร์มเอกสารทางกฎหมายให้สอดคล้องกับกิจกรรมขององค์กร (TOR 4.3.4.2))

สิ่งส่งมอบงานโครงการ (Project Deliverables)

การส่งมอบงาน จำนวน 3 งวด

3

งวดที่ 3
ภายใน 240 วัน
นับถัดจากวันลงนามในสัญญา

งวดที่ 3 : กำหนดส่งมอบ 21 กรกฎาคม 2565 (กำหนดส่งมอบก่อน 7 วัน : 14กรกฎาคม 2565)

(16) ตรวจสอบและให้คำแนะนำเกี่ยวกับเอกสารทางกฎหมายที่จำเป็นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (TOR 4.3.4.3))

(17) การประเมินความเสี่ยงพื้นฐานตามกฎหมาย (TOR 4.3.5)

(18) ทบทวนรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ฉบับสมบูรณ์ (TOR 4.3.5.1)

(19) รายงานการวิเคราะห์ช่องว่างและข้อบกพร่องพื้นฐาน (Basic Gap Analysis Report) (TOR 4.3.5.2)

(20) จัดกิจกรรมให้ความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (TOR 4.4)

5. กรอบแนวคิด มาตรฐาน และแนวปฏิบัติอ้างอิง

แนวคิดในการดำเนินการ

ที่ปรึกษากำหนดกรอบการดำเนินงาน โดยนำมาตรฐานสากลที่เกี่ยวข้องมาปรับใช้ในการกำหนดแนวทางการดำเนินงานในโครงการฯ ดังนี้

- กฎเกณฑ์ General Data Protection Regulation (GDPR) และแนวปฏิบัติที่ประกาศใช้ในกลุ่มประเทศยุโรป
- มาตรฐานสากล ISO/IEC 27701 Privacy Information Management (Aug. 2019)
    - ดำเนินการตามข้อกำหนดกรอบการบริหารจัดการและมาตรการคุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานสากล ISO 29100 Privacy Framework (Implementation)
- มาตรฐาน NIST Privacy Framework และ NIST Cybersecurity Framework

ทั้งนี้ สามารถให้คำปรึกษาในการปรับใช้มาตรฐานด้านเทคโนโลยีสารสนเทศ ที่อาจเกี่ยวข้องกับการดำเนินการในด้านอื่นได้

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

หน้า ๕๒
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

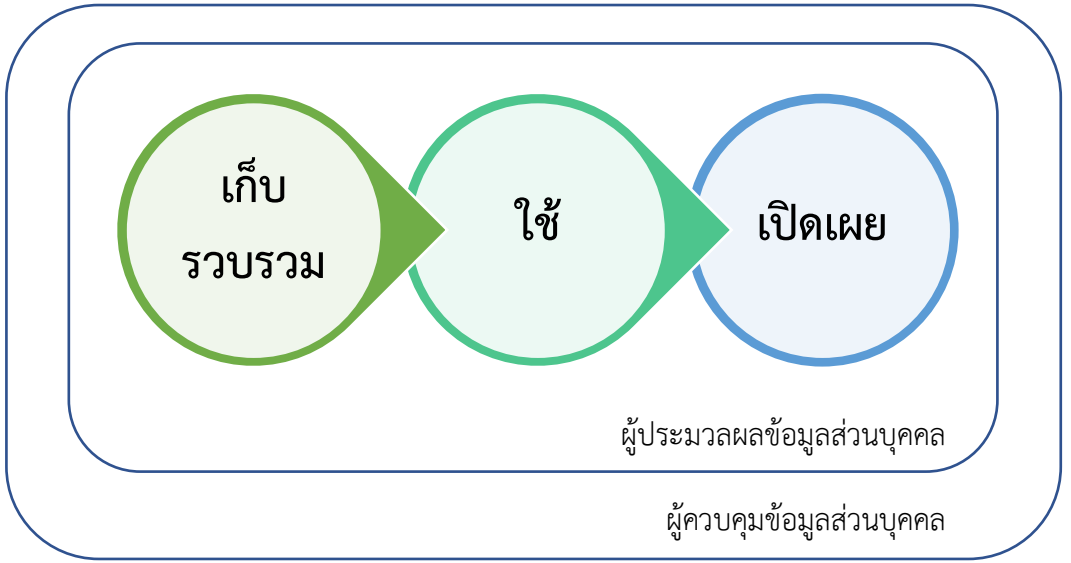
พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

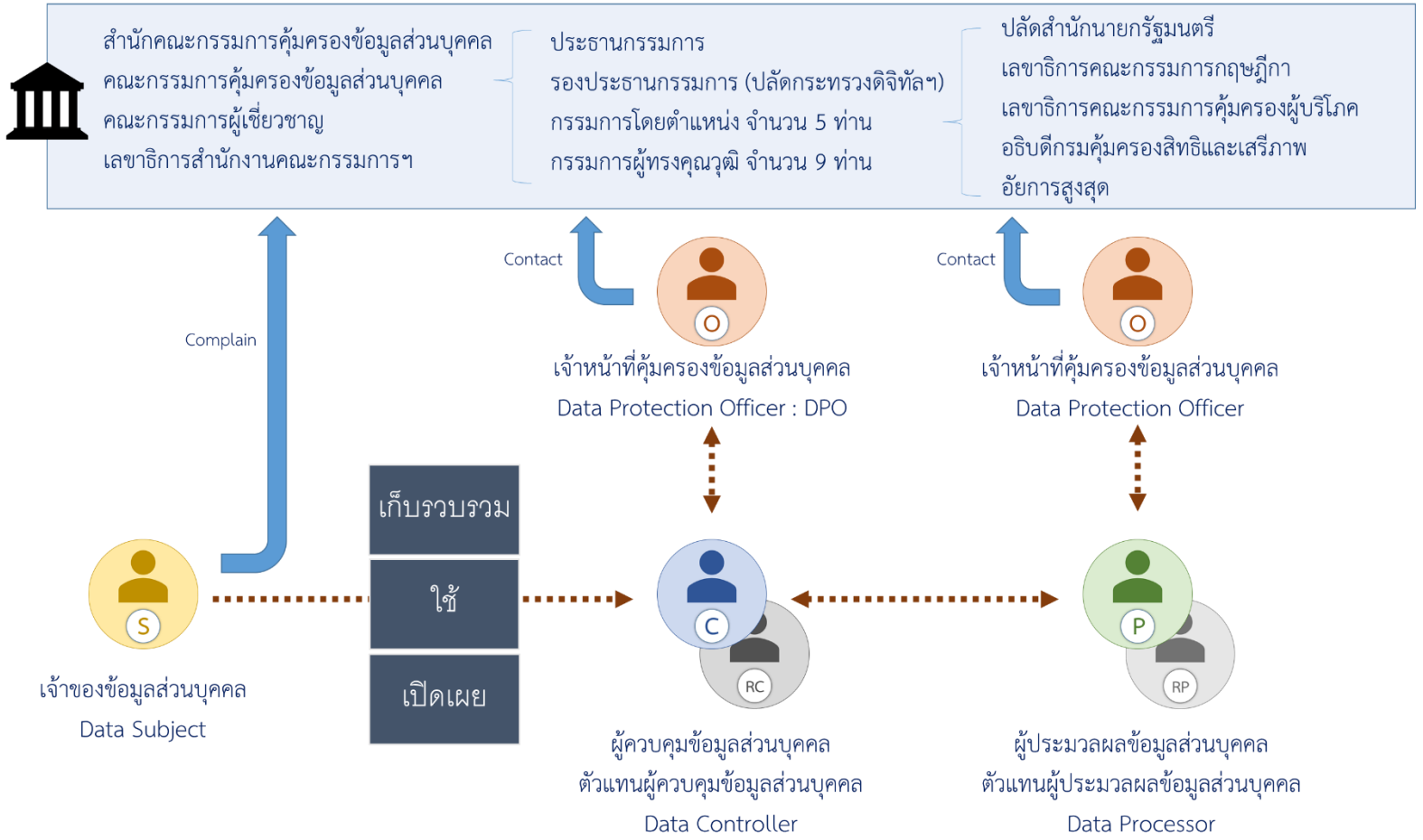
ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจาก การถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินสื้อดคล้องกบัเงื่อนไข ที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

พระราชบัญญัตินี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป



บทบาทและหน้าที่ตาม พ.ร.บ. หมวด3



ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

เป็นแนวทางการปฏิบัติเพิ่มเติมจาก ISO/IEC 27001:2013 เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ ISO/IEC 27701:2019 มีข้อกำหนดซึ่งมีความคล้ายคลึงกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก และสามารถนำมาใช้เป็นแนวทางปฏิบัติ เพื่อให้องค์กรดำเนินการได้สอดคล้องกับกฎหมายได้อย่างมีประสิทธิภาพมากขึ้น

มาตรฐาน ISO/IEC 27701:2019 ประกอบด้วยมาตรการรักษาความมั่นคงปลอดภัยข้อมูล ซึ่งระบุอยู่ในส่วน annex ของ ISO/IEC 27001:2013 และมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยส่วนที่เพิ่มเติมนั้นสามารถแบ่งได้ออกเป็น 2 ส่วน คือ

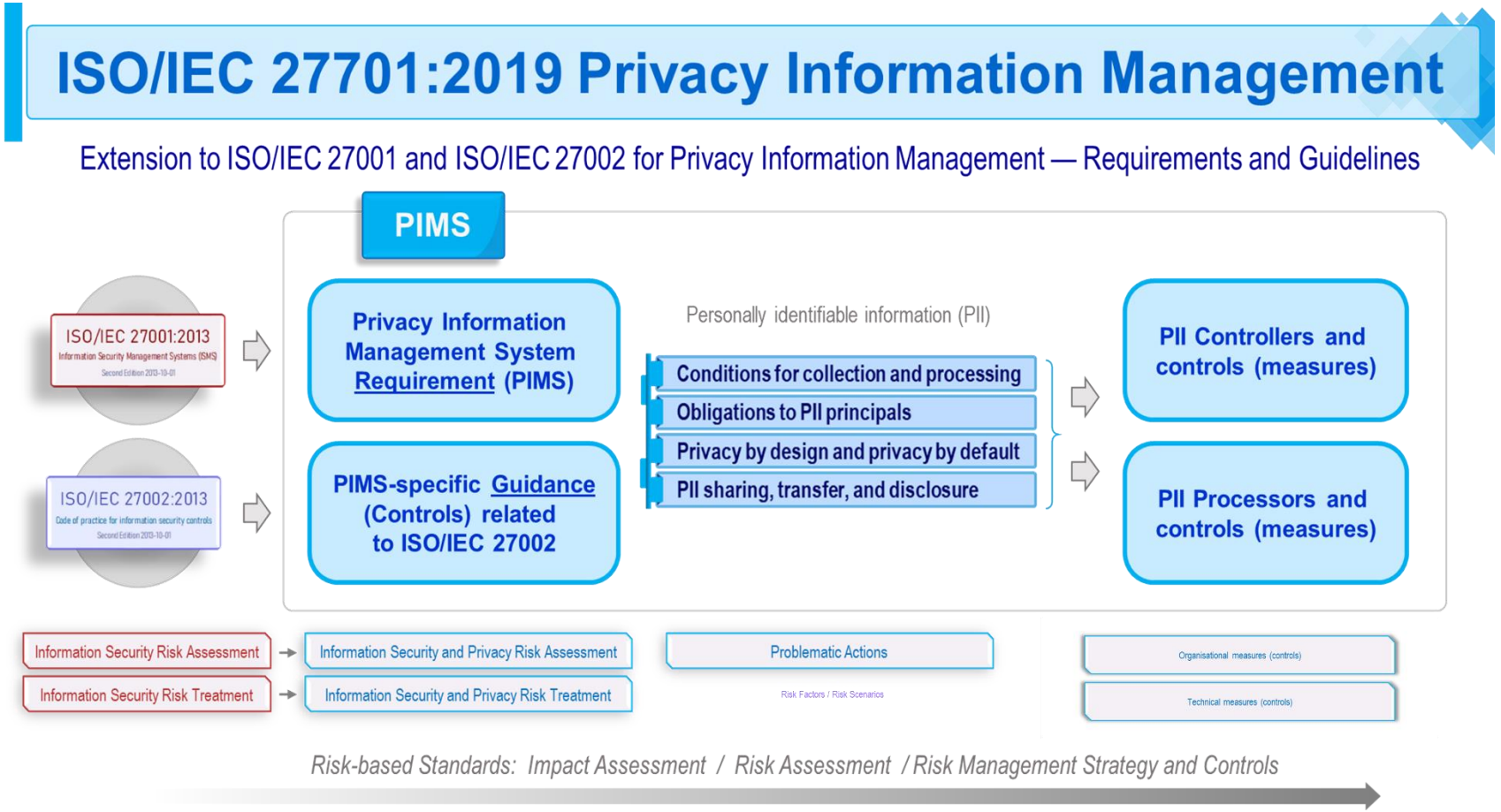
⌘ Additional ISO/IEC 27002 guidance for PII controllers

- ประกอบด้วยมาตรการและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การระบุฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities) การส่ง หรือโอนไปยังต่างประเทศ เป็นต้น

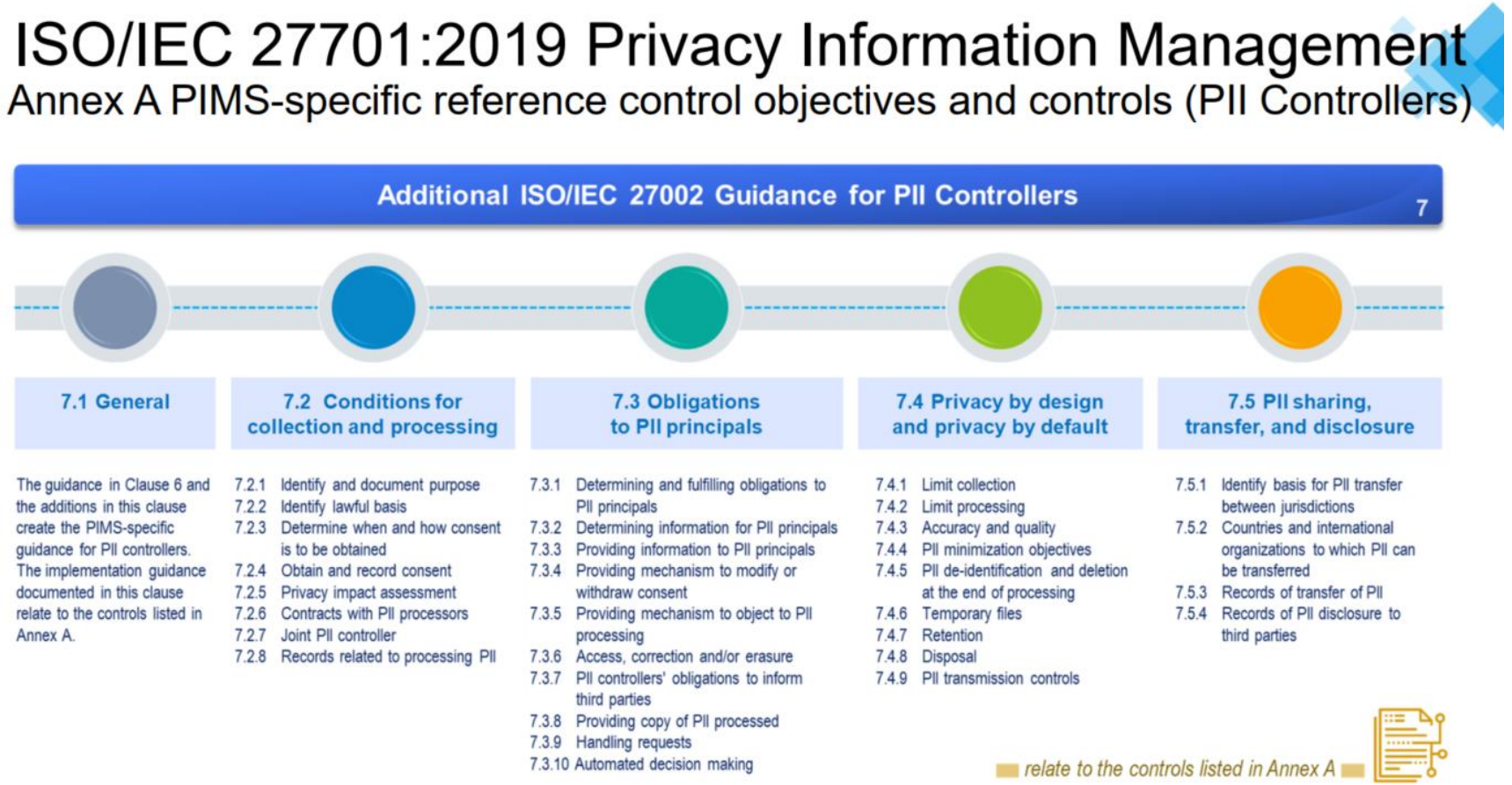
⌘ Additional ISO/IEC 27002 guidance for PII processors

- ประกอบด้วยมาตรการหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล เช่น การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities) การส่ง หรือโอนไปยังต่างประเทศ การปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้สัญญากับผู้ควบคุมข้อมูลส่วนบุคคล เป็นต้น

ความเกี่ยวข้องกับของมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) และมาตรฐานการบริหารจัดการข้อมูลส่วนบุคคล (ISO/IEC 27701)



แนวทางการกำหนดการควบคุมของ PII Controller ตามมาตรฐาน ISO/IEC 27701



แนวทางการกำหนดการควบคุมของ PII Processors ตามมาตรฐาน ISO/IEC 27701

ISO/IEC 27701:2019 Privacy Information Management

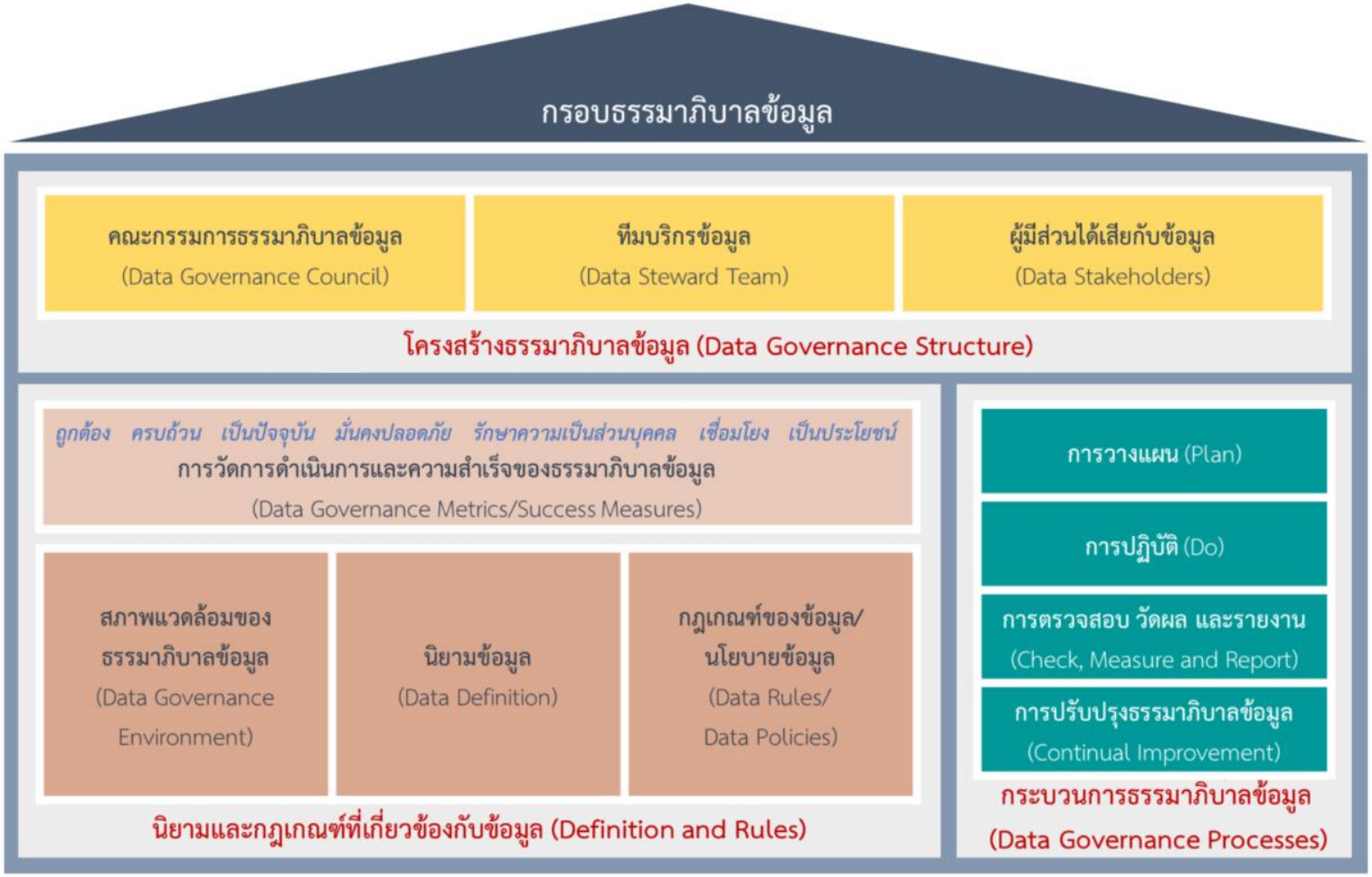
Annex B: PIMS-specific reference control objectives and controls (PII Processors)

Additional ISO/IEC 27002 Guidance for PII Processors 8

8.1 General	8.2 Conditions for collection and processing	8.3 Obligations to PII principals	8.4 Privacy by design and privacy by default	8.5 PII sharing, transfer, and disclosure
The guidance in Clause 6 and the additions of this clause create the PIMS-specific guidance for PII processors. The implementation guidance documented in this clause relate to the controls listed in Annex B.	8.2.1 Customer agreement 8.2.2 Organization's purposes 8.2.3 Marketing and advertising use 8.2.4 Infringing instruction 8.2.5 Customer obligations 8.2.6 Records related to processing PII	8.3.1 Obligations to PII principals	8.4.1 Temporary files 8.4.2 Return, transfer or disposal of PII 8.4.3 PII transmission controls	8.5.1 Basis for PII transfer between jurisdictions 8.5.2 Countries and international organizations to which PII can be transferred 8.5.3 Records of PII disclosure to third parties 8.5.4 Notification of PII disclosure requests 8.5.5 Legally binding PII disclosures 8.5.6 Disclosure of subcontractors used to process PII 8.5.7 Engagement of a subcontractor to process PII

relate to the controls listed in Annex B

โครงสร้างกรอบธรรมาภิบาลข้อมูล



6. เอกสาร PDPA เทียบกับกฎหมายแต่ละมาตรา

เอกสาร PDPA เทียบกับกฎหมายแต่ละมาตรา

รายการเอกสาร	มาตรา
เอกสารหน้าที่ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)	มาตรา 42
แบบฟอร์มรายการกิจกรรมที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล (Data Inventory)	มาตรา 39,40
เอกสารนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของส่วนกลาง ซึ่งครอบคลุมทั้งในส่วนที่เกี่ยวข้องกับลูกค้า และพนักงาน	หมวด 2 และ หมวด 3
เอกสารนโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)	มาตรา 22 และมาตรา 23
นโยบายการแยกประเภทของข้อมูลส่วนบุคคล (Personal Data Classification Policy) และ/หรือ ขั้นตอนการจัดลำดับชั้นของข้อมูลส่วนบุคคล (Personal Data Classification Procedure)	มาตรา 26
นโยบายในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)	หมวด 2
นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)	มาตรา 40

เอกสาร PDPA เทียบกับกฎหมายแต่ละมาตรา

รายการเอกสาร	มาตรา
นโยบายการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก หรือการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่น (Third Parties / Cross Border Data Transfer Policy) (ถ้ามี)	มาตรา 28 และมาตรา 29
ขั้นตอนปฏิบัติการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure)	มาตรา 19 และมาตรา 20
ขั้นตอนหรือแนวปฏิบัติการแจ้งสิทธิของเจ้าของข้อมูลส่วน (Data Subject Right Management) และแบบฟอร์มการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล	มาตรา 19
ขั้นตอนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment (DPIA) Procedure)	ประกาศตามกฎหมายลูก เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
กระบวนการจัดการปัญหาเมื่อเกิดข้อร้องเรียน และ/หรือ การละเมิด การรั่วไหล ของข้อมูลส่วนบุคคล (Personal Data Breach Procedure)	มาตรา 37 (4)
เอกสาร Data Processing Agreement	ตามมาตรา 40

ความต้องการการสนับสนุนต่างๆ จากสำนักงานปลัดกระทรวงพาณิชย์

- สำนักงานปลัดกระทรวงพาณิชย์ จะต้องจัดตั้งคณะทำงานเพื่อรับผิดชอบในการทำงานตามคำแนะนำของบริษัทฯ ตลอดจนประสานงานกับส่วนงานต่างๆ ที่เกี่ยวข้องภายใน
- ผู้บริหารของ สำนักงานปลัดกระทรวงพาณิชย์ จะต้องให้ความเห็นในประเด็นต่างๆ ในระยะเวลาที่เหมาะสมและทันต่อเวลา
- กรณีที่บริษัทฯ ไปปฏิบัติงานที่อาคารสำนักงานของ สำนักงานปลัดกระทรวงพาณิชย์ ขอความร่วมมือสำนักงานปลัดกระทรวงพาณิชย์จัดเตรียมสถานที่ และสิ่งอำนวยความสะดวกสำหรับการปฏิบัติงานของบริษัทฯ
- บริษัทฯ จะเข้าดำเนินงานที่ สำนักงานปลัดกระทรวงพาณิชย์ ในช่วงเวลาทำการของ สำนักงานปลัดกระทรวงพาณิชย์ หรือใช้การทำงานผ่านระบบ VDO Conference ตามที่ได้ตกลงร่วมกันในแผนการดำเนินโครงการกับสำนักงานปลัดกระทรวงพาณิชย์
- หากสถานการณ์ COVID-19 มีความร้ายแรงตามประกาศของหน่วยงานราชการ บริษัทฯ จะหลีกเลี่ยงในการเข้าทำงานสำนักงานปลัดกระทรวงพาณิชย์ และจะทำงานผ่านระบบ VDO Conference เท่านั้น

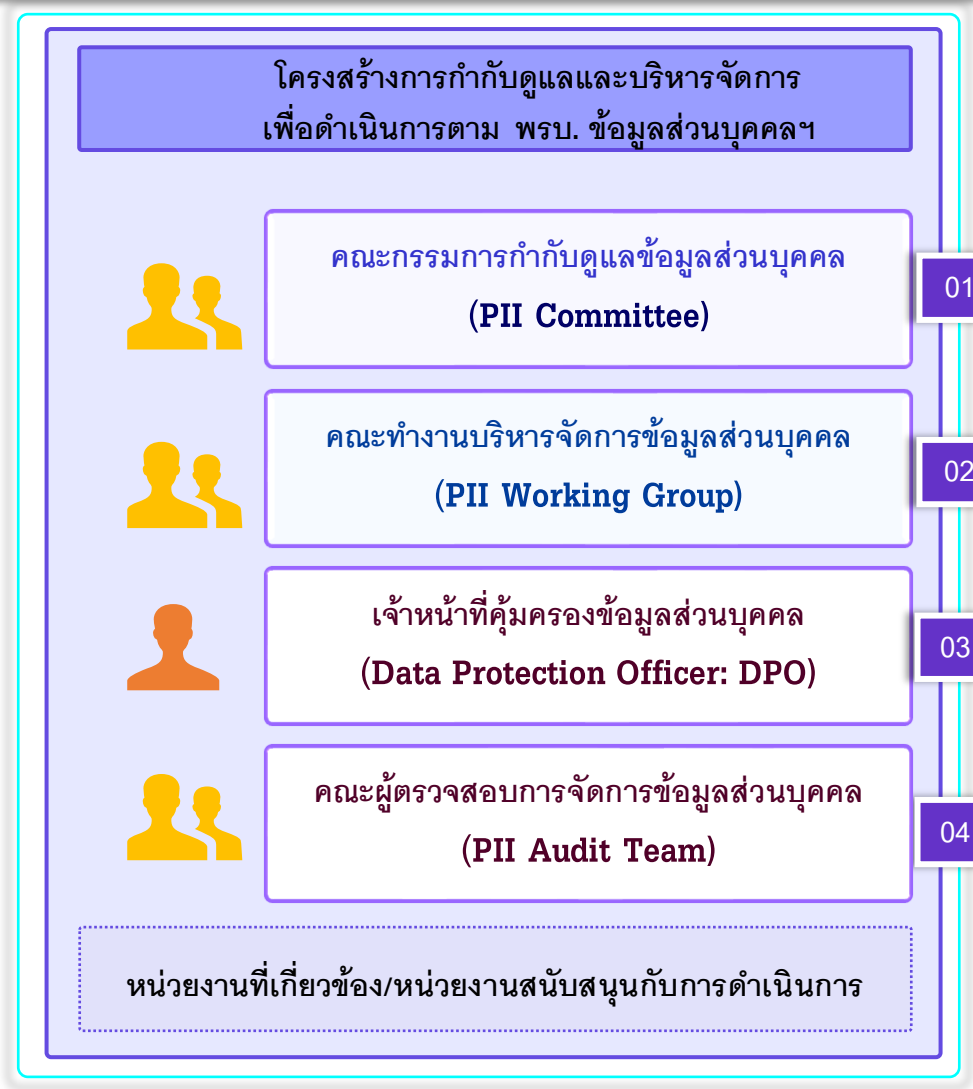
7. แผนดำเนินงานโครงการ (Project Plan)

	TOR	Task Name	วันที่	Responsible	Output
			23 พ.ย. 65		
0	4.1		23-30 พ.ย. 65	SCH, YLA, PRU	เอกสาร Project plan & Action plan
1	6.2		6 ธ.ค. 65	SCH, YLA, PRU	รายงานความก้าวหน้าการดำเนินงาน (Progress Report) ประจำเดือน
2	4.3.1	**คพส แต่งตั้งคณะกรรมการ คณะทำงาน (Working Team) คณะผู้ตรวจสอบและ DPO**	12 ธ.ค.65 - 6 ม.ค. 66	**ทีมที่ปรึกษา และ สป.พณ**	(ร่าง) คำสั่งแต่งตั้งคณะทำงาน
3		**คำนินการร่วมกับบุคลากรของ สป.พณ ในการกำหนดแนวทางการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** (Data Protection Officer)	1-6 มี.ค. 65	**ทีมที่ปรึกษา และ สป.พณ**	(ร่าง) หน้าที่ความรับผิดชอบของ DPO
4	4.2.1	**เร่งแก้ไขธรรมาภิบาลข้อมูลภาครัฐ**	19 ธ.ค.65 - 6 ม.ค. 66	MPA, YLA, PRU	เอกสารการศึกษา ด้านวพ การวิเคราะห์ และการพัฒนาปรับปรุงให้ใช้ระดับและประเมินความเหมาะสมด้านธรรมาภิบาลข้อมูลภาครัฐและด้านนโยบาย กฎ ระเบียบ ของ สป.พณ ตามที่รัฐกำหนด
5	4.2.2	**เป็นไปตามแนวทางที่ภาครัฐกำหนด**	19 ธ.ค.65 - 6 ม.ค. 66	MPA, YLA, PRU	
6	4.2.3	**ทบทวนปรับปรุงให้ชัดเสนอแนะ ด้านนโยบาย กฎ ระเบียบ และเอกสารที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ของสำนักงานปลัดกระทรวงพาณิชย์ ตามที่รัฐกำหนด**	19 ธ.ค.65 - 6 ม.ค. 66	MPA, YLA, PRU	
7	4.3.2	**คำนินการประเมินสถานกระบวนงานข้อมูลส่วนบุคคล** (Gap Analysis Assessment) **ของ สป.พณ.** - จัดทำ Gap กฎหมายตามมาตร - จัดทำ Gap ภาพรวม IT	26 ธ.ค. 65 - 10 ก.พ. 66	MPA, YLA, PRU	เอกสารประเมินสถานะกระบวนงานข้อมูลส่วนบุคคล (Gap Analysis Assessment)
8	4.3.3.1	**ครีแจ้งเจ้าหน้าที่ที่เกี่ยวข้อง จำนวน 1 วัน (6 ชั่วโมง)**	30 ม.ค. 65- 10 ก.พ. 66	SCH, KTU, PRU	เอกสารการชะแนะและผลการชะแนะ
9	4.3.3.1 4.3.3.2	**ณ์กลุ่ม (Focus Group) จำนวน 5ง (Session ละ 3 ชม.) ในหัวข้อต่อไปนี้**	26 ธ.ค. 65 - 10 ก.พ. 66	**ทีมที่ปรึกษา และ สป.พณ**	Data Inventory ทรัพ RoPA ของแต่ละหน่วยงาน (ตามรายการด้านล่าง)
		คำแนินการให้คำแนะนำการรวมรวมข้อมูลที่จากรกรรมที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อจัดทำรายการกิจกรรมที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล (Data Inventory ทรัพ RoPA) คำแนินการพร้อม ๆ กัน Workshop ตามแต่ละหน่วยงาน			
			26 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองกลาง
			27 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองตรวจราชการ
			28 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองบริหารการคลัง
			29 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองบริหารการพาณิชย์ปฏิบัติการ
			30 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองบริหารทรัพยากรบุคคล
			31 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกองยุทธศาสตร์และแผนงาน
			32 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
			33 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสถาบันการพาณิชย์จังหวัดปทุมธานี
			34 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกลุ่มกฎหมาย
			35 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกลุ่มตรวสอบภายใน
			36 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของกลุ่มพัฒนาระบบบริหาร
			37 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของศูนย์ปฏิบัติการต่อต้านการทุจริต
			38 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสำนักงานรัฐมนตรี
			39 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสำนักงานพาณิชย์จังหวัดทั่วกรมฯ (77 จังหวัด)
			40 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสำนักงานพาณิชย์ในต่างประเทศ ณ กรุงวอชิงตัน ดี.ซี
			41 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสำนักงานพาณิชย์ในต่างประเทศ ณ กรุงบรัสเซลส์
			42 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของสำนักงานพาณิชย์ในต่างประเทศ ณ กรุงปักกิ่ง
		คำนาทรัพย์สินทางปัญญาโลก (เพิ่มวาง)	43 ธ.ค. 65 - 10 ก.พ. 66	ทีมที่ปรึกษา และ สป.พณ	Data Inventory ของคณะผู้แทนถาวรไทยประจำองค์การการค้าโลกและองค์การทรัพย์สินทางปัญญาโลก (เพิ่มวาง)
10	4.3.3.2	**มินความเสี่ยงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล**	30 ม.ค. 65- 6 ก.พ. 66	YLA, MPA, PRU	เอกสารชุดคำถาม (Questionnaire) และเอกสารประเมินความเสี่ยงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
11	4.3.3.6	**รวมผลข้อมูลส่วนบุคคล** (RoPA Report)	30 ม.ค. 66- 6 ก.พ. 66	**ทีมที่ปรึกษา**	รายงานนิติศึกษาการจัดทำรวมการประมวลผลข้อมูลส่วนบุคคล (RoPA Report)
12	4.3.4.1	**คำนินการร่วมกับคณะทำงานของ สป. พณ. ในการร่างเอกสารนโยบายหรือแนวปฏิบัติหรือแบบฟอร์ม ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล** 1) นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) 2) หนังสือให้ความยินยอมแบบมาตรฐาน (Consent Form) 3) ขั้นตอนปฏิบัติในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure) 4) ประกาศความเป็นส่วนตัว (Privacy Notice) 5) ข้อตกลงการประมวลผลข้อมูลแบบมาตรฐาน ที่ทำเป็นตามรูปแบบระดับและกิจกรรม (Data Processing Agreement) 7) กระบวนการจัดการปัญหาเมื่อเกิดข้อขัดข้องเสียน และหรือ การละเมิดการชั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach Procedure) 8) เอกสารบันทึกการแจ้งเหตุละเมิด 9) จัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement) 10) นโยบายคุกกี้ (Cookies Policy) 11) เอกสารที่เกี่ยวข้องกับกระบวนการบริหารงานบุคคล 12) แนวทางการกำกับและติดตามและการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลแนวทางการตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล	27 ก.พ.66- 30 เม.ย. 66	YLA, MPA, PRU	1) นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) 2) หนังสือให้ความยินยอมแบบมาตรฐาน (Consent Form) 3) ขั้นตอนปฏิบัติในการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure) 4) ประกาศความเป็นส่วนตัว (Privacy Notice) 5) ข้อตกลงการประมวลผลข้อมูลแบบมาตรฐาน ที่ทำเป็นตามรูปแบบระดับและกิจกรรม (Data Processing Agreement) 7) กระบวนการจัดการปัญหาเมื่อเกิดข้อขัดข้องเสียน และหรือ การละเมิดการชั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach Procedure) 8) เอกสารบันทึกการแจ้งเหตุละเมิด 9) จัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement) 10) นโยบายคุกกี้ (Cookies Policy) 11) เอกสารที่เกี่ยวข้องกับกระบวนการบริหารงานบุคคล 12) แนวทางการกำกับและติดตามและการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลแนวทางการตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล
13	-	**n Policy/Procedure)**	6-17 มี.ค. 66	YLA, MPA, PRU	Data Classification Policy/Procedure
14	-	**ข้อมูลส่วนบุคคล** (Data Subject Right Management)			เอกสารระบบงานการบริหารจัดการข้อมูลใช้สิทธิ์เจ้าของข้อมูลส่วนบุคคล (Data Subject Right Management)
15	-	**source/Third Parties Policy)**			แนวปฏิบัติการควบคุมผู้ให้บริการภายนอก (Outsource/Third Parties Policy)
16	-	**ทศ** (Cross-Border Transfer Procedure)			เอกสาร กระบวนการควบคุมการส่งข้อมูลไปยังต่างประเทศ (Cross-Border Transfer Procedure)
17	-	**ทำลายข้อมูล** (Data Retention/ Disposal Policy)			นโยบาย และแนวปฏิบัติการจัดเก็บข้อมูลและการทำลายข้อมูล(Data Retention/ Disposal Policy)
18	4.3.4.2	**วยให้สอดคล้องกับกิจกรรมขององค์กร**	6 -30 มิ.ย. 66	YLA, MPA, PRU	เอกสารที่ได้รับการปรับปรุงแก้ไขให้สอดคล้องกับกิจกรรมขององค์กร ตามที่TOR กำหนด
19	4.3.4.3	**วยที่จำเป็นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล**	6 -30 มิ.ย. 66	YLA, MPA, PRU	เอกสารตรวจสอบและให้คำแนะนำที่เกี่ยวกับเอกสารที่จำเป็นตามกฎหมายในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
20	4.3.5	%A & Risk Assessment)	6 - 31 มี.ค. 66	SCH, KTU, PRU	เอกสารการประเมินผลกระทบและความเสี่ยง (PIA & Risk Assessment)
21	4.3.5.1	**ทบทวนตรวจสอบบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล** (RoPA) **และจัดทำรายงานบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล** (RoPA Report) **ฉบับล่าสุด**	15 พ.ค. 66 - 23 มิ.ย. 66	YLA, MPA, PRU	บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) และจัดทำรายงานบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA Report) ฉบับล่าสุด
22	4.3.5.2	**คำนินการจัดทำรายงานการวิเคราะห์ช่องว่างและข้อบกพร่องพื้นฐาน** (Basic Gap Analysis Report) 1) คำนินการประเมินความเสี่ยงด้านความเป็นส่วนตัว (Privacy Risk) 2) คำนินการประเมินความเสี่ยงด้านความปลอดภัย (Security Risk)	27 ก.พ. 66- 21 เม.ย. 66	YLA, MPA, PRU	รายงานการวิเคราะห์ช่องว่างและข้อบกพร่องพื้นฐาน (Basic Gap Analysis Report)
23	6.3	**ประชุมรายงานความก้าวหน้าการดำเนินงาน** (Progress Report) **ประจำเดือน (กำหนดนัดหมายนำเสนอ** Powerpoint **รายงานความก้าวหน้าประจำเดือน)** *หาวิธีนัดหมายมายากอง	**ประจำทุกเดือน**	SCH, YLA, PRU, Working Team	powerpoint รายงานความก้าวหน้าการดำเนินงาน ประจำเดือน
24	-	**แห้งหมด 3 ครั้ง)**	1 สัปดาห์ก่อนถึงวันส่งมอบงาน	SCH, YLA, PRU, Working Team	
25	4.3.5.2	**งข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕**	26 มิ.ย. 66 - 3 ก.ค. 66	SCH, KTU, PRU	เอกสารจัดทำระบบให้ความรู้ที่เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ต่อเอกสารการอบรมให้ความรู้
26	-	**ใครงการฯ**	19-21 มิ.ย. 66	SCH, KTU, PRU	เอกสารที่ได้รับการอนุมัติและประกาศใช้
27	-	**ติงานจริง** (Policy/Procedure Improvement)	10- ก.ค. 66	SCH, KTU, PRU	เอกสารตรวสคุณที่ปรับปรุงแก้ไขให้เหมาะสมกับการนำไปปฏิบัติงานจริง
28	-	**แนะสอบภายนอก (Internal Audit/Guidance ISO27701)**	26-30 มิ.ย. 66	SCH, KTU, PRU	เอกสารแนวปฏิบัติการตรวจสอบภายใน และข้อเสนอแนะตามมาตรฐานสากล (Internal Audit/Guidance ISO27701)
29	-	**ร (Policy/Procedure Training)**	3-14 ก.ค. 66	SCH, KTU, PRU	เอกสารการอบรมและผลการอบรม
		กำหนดการส่งมอบงาน	**กำหนดส่งมอบ**	**ส่งมอบจริง (ก่อน 7 วัน)**	
		งวดที่ 1: 30 วัน	22 ธ.ค. 65	15 ธ.ค. 65	งานส่งมอบงวดที่ 1
		งวดที่ 2: 90 วัน	21 ก.พ. 66	14 ก.พ. 66	งานส่งมอบงวดที่ 2
		งวดที่ 3: 240 วัน	21 ก.ค. 66	14 ก.ค. 66	งานส่งมอบงวดที่ 3

Microsoft Excel Worksheet

8.ข้อเสนอแนะการจัดตั้งโครงสร้างการกำกับดูแลฯ

Example : PII Org. Chart



- Chairman of Board & Managing Director
- Senior Director, Corporate Planning
- Commercial Director
- Marketing & Business Development Director`

- Assistant Compliance Manager / Corporate Secretary
- Executive IT Manager
- Assistant HR Manager
- Executive Supply Chain Manager
- Executive Marketing, Sales Manager

- Compliance Manager
- OR Compliance Specialist
- OR Outsource

* Report directly to PII Committee

- Company internal auditor
- External auditor

ตัวอย่างหน้าที่รับผิดชอบ Steering Committee

ตัวอย่างหน้าที่รับผิดชอบ Steering Committee:

1. พิจารณาและอนุมัตินโยบาย และ แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. ส่งเสริม สนับสนุน ให้คำปรึกษาคณะทำงาน เพื่อให้การดำเนินการเป็นไปตามกรอบทิศทางตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงเป็นผู้ชี้นำการสร้างจิตสำนึกด้านการคุ้มครองข้อมูลส่วนบุคคลทั่วทั้งองค์กร
3. สนับสนุนทรัพยากรต่าง ๆ ในการปฏิบัติงาน ให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตัวอย่างหน้าที่รับผิดชอบ *Working Team*

ตัวอย่างหน้าที่รับผิดชอบ *Working Team*:

1. กำหนดนโยบาย และ แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อขออนุมัติประกาศใช้
2. ประสานงานกับหน่วยงานต่างๆ เพื่อให้รับทราบและปฏิบัติตามนโยบาย และ แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. ประเมินผลการจัดทำโครงการ ปรับปรุงมาตรการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และรายงานผลต่อผู้บริหาร

ข้อเสนอแนะในการแต่งตั้ง DPO

แนวทางในการแต่งตั้ง DPO:

1. แต่งตั้งพนักงานประจำที่ทำงานในปัจจุบัน
2. แต่งตั้งพนักงานประจำที่ทำงานในปัจจุบัน และจ้างที่ปรึกษาภายนอก
3. จ้างพนักงานสัญญาจ้าง (Contract)
4. จ้างนิติบุคคลภายนอกที่ให้บริการ DPO Outsource

ข้อเสนอแนะในการแต่งตั้ง DPO

รูปแบบการแต่งตั้ง	Pros	Cons
แต่งตั้งหรือจ้างพนักงานประจำ	- มีความเข้าใจในบริบทขององค์กรและธุรกิจ - สามารถประสานความร่วมมือภายในได้เป็นอย่างดี - ประหยัดค่าใช้จ่าย (กรณีไม่ได้จ้างพนักงานเพิ่ม)	- ขาดความเชี่ยวชาญในข้อกฎหมาย - ขาดความเชี่ยวชาญในด้านความมั่นคงปลอดภัย - มีความเสี่ยงในเรื่องของการลาออก - อาจจะมีประเด็นในเรื่องของ Conflict of Interest
จ้างในรูปแบบ Outsource (Turnkey)	- มีความเป็นกลาง และอิสระ ไม่มี Conflict of Interest - มีความเชี่ยวชาญทั้งในด้านของข้อกฎหมาย และด้านความมั่นคงปลอดภัย (ในกรณีจ้างนิติบุคคล หรือกลุ่มบุคคล) - ไม่มีปัญหาในเรื่องของการลาออก และสามารถเปลี่ยนได้ในกรณีที่ให้บริการต่ำกว่ามาตรฐาน - ไม่มีค่าใช้จ่ายในการฝึกอบรมเพิ่ม - มีประกันวิชาชีพ เช่น Professional Insurance (ในบางบริษัท)	- ค่าใช้จ่ายสูงกว่าการจ้างพนักงานประจำ - มีความเข้าใจในบริบทขององค์กรและธุรกิจน้อยกว่า - ประสิทธิภาพในการประสานงานน้อยกว่าพนักงานประจำ - ไม่ได้เข้ามานั่งทำงานประจำ (ขึ้นกับเงื่อนไขที่ตกลง) - ปัจจุบันมีผู้ให้บริการจำนวนน้อยมาก

ตัวอย่างหน้าที่รับผิดชอบ Audit Team

ตัวอย่างหน้าที่รับผิดชอบ Audit Team:

1. ดำเนินการตรวจสอบความถูกต้องของการทำงานของ DPO
2. ดำเนินการตรวจสอบแนวปฏิบัติและนโยบายต่างๆ ให้สอดคล้องตามตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. ดำเนินการช่วยเหลือ DPO ตรวจสอบความถูกต้องของการจัดเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคล

ถาม-ตอบ