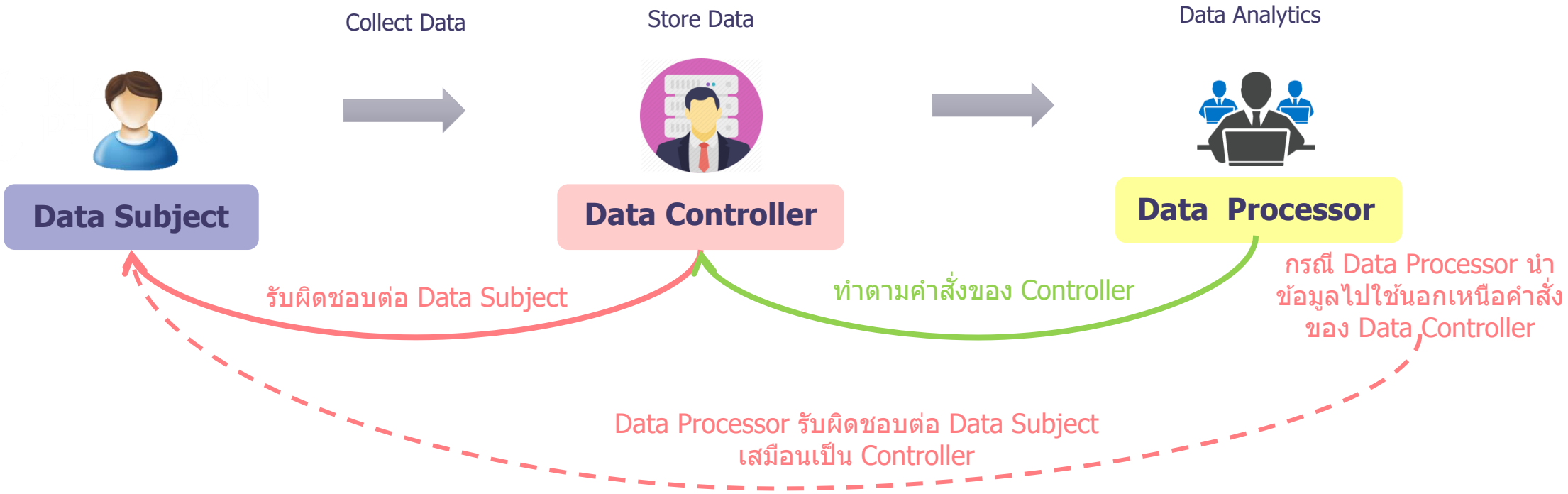
KIATNAKIN PHATRA

Compliance Training Program

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562

Data Controller & Data Processor : Overview



"คนที่ข้อมูลชี้ไปที่ตัวบุคคลนั้น"

"หน่วยงานภาครัฐ/เอกชน ที่เก็บรวบรวมข้อมูลแล้วนำไปใช้ประโยชน์ หรือนำข้อมูลไปส่งต่อหรือเปิดเผยต่อไป"

"นิติบุคคล หรือ บุคคล ที่เก็บรวบรวม ใช้ เปิดเผยข้อมูล หรือนำเอาข้อมูลส่วนบุคคล จาก Data Controller ไปใช้เพื่องานของ Data Controller"

ผู้มีหน้าที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

Data Controller

- **หน้าที่ในการแจ้งข้อมูล**
  - วัตถุประสงค์ในการเก็บรวบรวมข้อมูล
  - ฐานที่ชอบด้วยกฎหมาย
  - ประเภทข้อมูล
  - เปิดเผยให้กับบุคคลที่สามหรือไม่
  - รายละเอียดการโอนข้อมูลส่วนบุคคล
  - ระยะเวลาในการเก็บข้อมูลส่วนบุคคล
  - สิทธิต่างๆ ของเจ้าของข้อมูล
- **หน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูล**
- **หน้าที่ในการแจ้งกรณีข้อมูลส่วนบุคคลรั่วไหล**
  - แจ้งแก่ สนง.คุ้มครอง**ภายใน 72 ชั่วโมง**นับแต่ได้ทราบ เว้นแต่เหตุที่เกิดไม่ก่อให้เกิดความเสี่ยงใดๆ ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
  - แจ้งแก่ เจ้าของข้อมูลส่วนบุคคล
- **หน้าที่ในการลบข้อมูลส่วนบุคคล**
- **หน้าที่ในการบันทึกรายการ**
- **หน้าที่ในการจัดให้มีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล**

Data Processor

- **ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น**
- **จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม**
- **จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล**
- **แจ้งเหตุละเมิดให้ Data controller ทราบโดยไม่ชักช้า**

Data Protection Officer (DPO)

- **ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**
- **ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**

หน่วยงานที่ทำหน้าที่กำกับดูแล

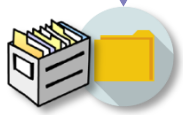
- **สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
- **คณะกรรมการผู้เชี่ยวชาญ**

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน

ผู้ควบคุมข้อมูลส่วนบุคคลควรตรวจสอบให้รู้ว่าในองค์กรมีกิจกรรมใดบ้างที่ใช้ข้อมูลส่วนบุคคล และแต่ละกิจกรรมนั้นมีวัตถุประสงค์อย่างไร เพื่อให้สามารถจัดทำมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งอาจกำหนดขั้นตอนการตรวจสอบกิจกรรมโดยการทำ Data Discovery ภายในองค์กร

Data Discovery

การสำรวจกิจกรรมที่ใช้ข้อมูลส่วนบุคคล



Asset

ฐานข้อมูล
สถานที่เก็บข้อมูลส่วนบุคคลที่เรานำข้อมูลทั้งในรูปแบบ Digital File หรือ กระดาษ ไปจัดเก็บรักษาบันทึกไว้ที่ใดบ้าง (Data Inventory)

Processing Activities

กิจกรรมการประมวลผล
กิจกรรมอะไรบ้างที่มีการนำข้อมูลไปใช้งาน และใช้อย่างไร มี Control ที่เพียงพอแล้วหรือไม่

Entities

หน่วยงานภายในองค์กร
คู่ค้า / Outsource
ผู้เกี่ยวข้องที่มีกิจกรรมนำข้อมูลไปประมวลผลซึ่งอาจมีความสัมพันธ์ในการใช้ข้อมูลร่วมกัน หรือมีการส่งต่อให้อีก Entities ซึ่งรวมถึงการส่งขอมูลออกไปภายนอก เช่น Vendors

Security Measure

กำหนดมาตรฐานการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เหมาะสมเป็นมาตรฐาน

Example: Template Data Discovery

No.	Process	Channel	Data Source	Data Subject	Data Type	Purpose of Process	Data Retention	Data transfer	Lawful Processing	Data Recipients	Relate System	Relate Document	BU Actions
001	การกรอกแบบสอบถาม	RM PB/Branch	Direct	Customer	Personal Details Contact Details	เพื่อเป็นข้อมูลทำกิจกรรมการตลาด	3 ปี	none	Consent	PB Marketing RM PB , Branch	Share drive	แบบสอบถาม Excel file บันทึกผลแบบสอบถาม	ด้านการดูแลไฟล์ข้อมูล 1. BU จัดเก็บข้อมูล File Excel ไว้ที่ SharePoint 2. กำหนดสิทธิ์ในการเข้าถึงไฟล์ 3. กำหนดระยะเวลาในการจัดเก็บข้อมูล 4.จัดทำบันทึกการจัดเก็บข้อมูล 5.จัดทำบันทึกการทำลายข้อมูล ด้านการดูแลข้อมูลเอกสาร 1. ดำเนินการเข้าแฟ้ม ระบุระดับชั้นความลับ 2. จัดเก็บเข้าตู้ที่มีกุญแจ
002	โอนเปลี่ยน Selling Agent	RM PB & RM Branch	Direct	Customer	Personal Details, Account Details (รายละเอียดของบัญชีกองทุนที่ทำธุรกรรม), Transaction Details, Copy Document	Transaction Processing	1 ปี	None	Contract	Controller (P-Asset), Selling Agent ผู้รับโอน	SMF, Share Point, ECM, Office365 (E-mail),MES	ใบคำขอโอนหน่วยลงทุน, สำเนาเอกสารแสดงตน	ด้านการดูแลข้อมูลเอกสาร 1. ระหว่างรอนำส่งจัดเก็บในลิ้นชักที่มีกุญแจ 2. กรณีข้ามวันจัดเก็บไว้ในตู้เซฟ ด้านการนำส่งเอกสาร ให้ Operation/KKPS 1. บันทึกทะเบียนนำส่งเอกสาร กำหนดสิทธิ์ในการเข้าถึง 2. นำเอกสารใส่ซองปิดผนึกระหว่างการนำส่ง ด้านการนำส่งไฟล์ข้อมูล 1.Encrypt File ก่อนส่งไปยังทีมที่เกี่ยวข้อง 2. กำหนด Password และนำส่งแยกจากไฟล์ข้อมูล 3. Review นำส่งข้อมูลเฉพาะผู้ที่เกี่ยวข้อง

Example: การทำ Security Measures

1. NO Copying / Scan File, Photo capture and Save File beyond work procedure
2. Checklist and Control of Document Received / delivery
3. Process of received and delivery document NO using of Personal LINE /e-mail / computer
4. Register Log of delivered document/report
5. Arrange Confidentiality level of Document and file

10 Security Measures

6. Register log of destroy document
7. Destroy and use of physical document and files
8. Saving of files Using of One Drive/ Share Point/ User password / role and authority
9. Sending of electronic mails by encryption and masking of data and using Link
10. Delete of unidentified files form personal drive and One Drive / share point

Example: Security Measures Details

มาตรการการดำเนินการ
ในกรณีที่เป็นสำเนาเอกสารที่ใช้ระบุตัวตนลูกค้า เช่น บัตรประชาชน หรือ passport เมื่อได้รับมาจากลูกค้า ห้ามทำสำเนาเพิ่มโดยเด็ดขาด (Xerox, Scan File, Email, Save File, download, Print ถ่ายรูปด้วยมือถือ) เว้นแต่จะเป็นการเก็บเข้าระบบหรือ storage ของธนาคาร ตามกระบวนการทำงานปกติ หรือเป็นไปตามหลักเกณฑ์ที่ธนาคารกำหนด
จัดทำใบรับส่งเอกสาร หรือ checklist สำหรับการรับส่งเอกสารภายใน และภายนอกองค์กร ให้รวมถึงระบุประเภทเอกสารที่ต้องขอจากลูกค้าในแต่ละผลิตภัณฑ์ และให้ลูกค้าลงนาม โดยจะต้องมีกระบวนการตรวจสอบความถูกต้องครบถ้วนของเอกสาร และปิดผนึกให้เรียบร้อยเพื่อป้องกันการละเมิดหรือล่วงรู้ข้อมูลระหว่างทาง
การจัดส่งเอกสารผ่านช่องทางต่างๆ - ใส่ซองปิดผนึก ระบุผู้รับให้ชัดเจน - นำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจากธนาคารโดยส่งถึงลูกค้าเท่านั้น เว้นแต่จะได้รับอนุญาตเป็นกรณีๆ ไป - กรณีใช้ผู้ให้บริการภายนอก ต้องเป็นบริษัทที่ธนาคารกำหนดเท่านั้น - กรณีส่งผ่านไปรษณีย์ต้องส่งแบบปิดผนึก ระบุผู้รับอย่างเจาะจงและต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลอื่นเพิ่มเติม เช่นการปิดบังข้อมูลสำคัญบางส่วนหรือใช้บริษัทผู้ให้บริการที่ธนาคารกำหนดเท่านั้น - ต้องมีการติดตามสถานะของการจัดส่ง โดยเฉพาะกรณีที่เจ้าของข้อมูลมิได้เป็นผู้รับเอง - ห้ามใช้ LINE หรือ Email ส่วนตัว ในการปฏิบัติงานหรือการรับทำธุรกรรมใดๆ ที่มีข้อมูลลูกค้า และข้อมูลลับ หรือลับมากของธนาคาร ยกเว้นจะได้รับอนุญาตจากคณะกรรมการที่เกี่ยวข้องเป็นรายกรณี
จัดทำทะเบียนการให้ข้อมูลที่จัดอยู่ในชั้นลับหรือลับมาก เพื่อให้สามารถติดตาม ตรวจสอบได้
ระบุชั้นความลับของเอกสาร ได้แก่ การจัดทำป้ายเพื่อระบุชั้นความลับที่เอกสาร แฟ้ม และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรการบริหารจัดการข้อมูลตามระดับชั้นความลับ
ให้จัดทำทะเบียนบันทึกการทำลายเอกสาร และข้อมูลตามทะเบียน Data Inventory ซึ่งอาจอยู่ในรูปแบบเอกสารหรือไฟล์ทะเบียน
วิธีการทำลายข้อมูล - เอกสาร ใช้เครื่องย่อยเอกสารชนิดที่ไม่สามารถกลับนำกลับมาประกอบใหม่หรือฉีกเอกสารก่อนหย่อนลงก่อง หรือถุงบริษัทรับทำลายเอกสารที่ธนาคารกำหนด - ลบข้อมูลหรือทำลายข้อมูลตามประเภทสื่อบันทึกข้อมูลให้ไม่สามารถกู้คืนข้อมูลกลับมาใช้ได้อีก ตามหลักเกณฑ์ที่ธนาคารกำหนด - ห้ามใช้กระดาษ reuse ควร print แบบ 2 หน้าทุกครั้ง
บันทึกไฟล์งานใน One Drive, SharePoint หรือระบบงานที่ธนาคารจัดเตรียมไว้ให้เท่านั้น และ จัดเก็บโดยกำหนดวันที่ และกำหนดสิทธิ์การเข้าถึงไฟล์ใน Folder หรือข้อมูลในระบบ เฉพาะพนักงานที่เกี่ยวข้อง และต้องมีการเข้ารหัส (encrypt) ด้วย สำหรับข้อมูลลับมาก
กรณีส่งไฟล์ที่มีข้อมูลลับหรือลับมากระหว่างกันภายในองค์กร ให้จัดทำเป็น link และส่งให้ผู้ที่ต้องใช้ข้อมูลเข้ามาดูผ่าน link ดังกล่าว หากไม่สามารถดำเนินการดังกล่าวได้และต้องส่งเป็นไฟล์ ให้ดำเนินการ encrypt ไฟล์ก่อนส่งออกทุกครั้ง โดยขอให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) และส่งเฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น ในกรณีเป็นผู้รับไฟล์ให้ปฏิบัติตามข้อ 1 หรือ save โดยไม่เป็นไปตามที่กำหนด
ลบข้อมูลหรือไฟล์งานที่บันทึกอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์ เช่น Drive C, Drive D กรณีมีความจำเป็นต้องใช้ข้อมูลให้ย้ายไปเก็บอยู่ใน OneDrive หรือ SharePoint โดยข้อมูลใน OneDrive ซึ่งเป็น Drive ส่วนตัว หากอยากเก็บไฟล์งานไว้ใช้อ้างอิงให้ดำเนินการนำข้อมูลส่วนบุคคลออกก่อน และให้จัดเก็บได้ตามระยะเวลาที่ฝ่ายงานกำหนดไว้ในชีท Document Inventory หรือลบทิ้งเมื่อไม่ต้องใช้งานแล้ว
กรณีมีความจำเป็นต้องบันทึกไฟล์ที่มีข้อมูลส่วนบุคลออกมาใช้งานบน Drive C, Drive D เช่น การทำงานบน Microsoft Office Online ไม่รองรับ ให้ทำได้เฉพาะกรณีใช้เครื่องคอมพิวเตอร์ของธนาคารเท่านั้น และเมื่อทำงานเสร็จและได้บันทึกไฟล์เข้าไปใน One Drive หรือ SharePoint แล้ว ต้องลบไฟล์ที่บันทึกไว้ในเครื่องคอมพิวเตอร์ทุกครั้ง และหมั่นลบไฟล์ที่อยู่ในเครื่องทุกปี

Performance Verification Process

1. Self Test

- The head of the business unit selects the processes that are critical to audit and makes a self-test plan.

2. Warm Test

- Internal Audit and PDPA team check readiness Customer Service Points and Business Unit Processes (such as using a mystery shopper)
- If finds a gap, the business unit can improve the process to close that gap again.

3. Internal Audit

- The Audit Department operates according to the annual audit plan.

4. Update Board

- Report results to the board of directors

Check to ensure that the security of the information is sufficiently standardized.

Example GAP #1: Using of Social Medias for Client Information

GAP	Action	Target
Using personal LINE or other social media for sending/receiving client personal information	**Internal:** Using MS Team instead of LINE **External:** 1. IT creates MS Team Group for using with Vendors / Partners 2. Setup email for outsource staff (@kkpoutsource.com) 3. Develop Official LINE for Sale / Marketing / Dealer 4. Develop SMS link for prospect / customer to submit info/document to KKP	**Internal:** Q2'2021 **External:** 1/and 2) Set Group MS Team and Group email on request 3) Official Line (Line KKP Auto Connect) / email • AF - May 2021 4) SMS Link – Feb 2021

Example GAP #2: Own Device

GAP	Action	Target
• Marketing /Outsource uses own device to process cases (Data leak opportunities from 120 OS / month = 600 dealers /3600 customers = 4200 opportunities) • Staff request to use own devices • Develop Software to close the Gap on Staff's devices	• Explore to provide plug in application on device and register device under bank's standard and work on cloud bases, no save , no download • Treat on bank device standard • Explore solution and decided by Steering/Committee	**Internal:** Q2'2021

Example GAP #3: Data Leak & Data Breach

GAP	Action	Target
• Found approximately 5500 mails / week sent out to free mails which addresses are similar to staff's name. This lead to data leak	• Minimize back office staff's right on sending outside Mail.	Q2'2021
• Office365 E1 License isn't fully utilized	• IT provides user's manual i.e. create link to file in One Drive / SharePoint etc.	Q2'2021
• Need advance license (Office 365 E3 License) to prevent data leak. (NO forward, NO download attached file, recall email, set active period etc.)	• Data Steward did users survey and received 1900 requests for Office 365 E3 License. Need Biz Heads to review needs which related to client Info & outside mail	Q2'2021

Example GAP #4: Right to be forgotten / Data Destruction

GAP	Action	Target
• May not erase all personal information when clients exercise their right (data file / paper) on staff's computer	• Announce KKP Data Security Measure; data inventory to destroy paper, no unnecessary copies and no personal drive storage	Data Security Measure: 18 Jan 2021
• Cannot erase all personal information when clients exercise their right (voice file that stores in the systems / back up tape)	• Staff signs PDPA self-Certify	Q2'2021
	• Set data retention period for voice storage according to each Biz use cases	Q2'2021
	• Explore new Voice data structure with vendor to comply with PDPA requirement	Q2'2021

Data Protection – Data Leakage Channel

USB media

1. Use company asset only
2. Authorized by Group Head, under risk advise by DSC
3. *Use case had been defined
4. BU is responsible to control the media use regularly
5. Annual review by IT
6. Return media when transfer / resign
7. Data need to destroy when return

External Print

1. Print only in the office is standard
2. Non-office printer is block

Outside office print if need:

1. Fixed printer and less memory model
2. Authorized by Group Head
3. Pre-defined the accepted outside printer is for
   - Customer serving (Marketing, Dealer)
   - Large amount of document content (Legal)

*Other needs will be survey

4. Present “Less memory printer” & “qualified shedder machine” before authorize the use
5. IT verify the printer model to ensure its less memory before grant*

External Email

1. Block for Free email
2. Allow for Senior manager level & up
3. Below Senior manager level use under whitelist (specific recipient)*
4. EMS E3 is required for Sensitive user group

Laptop

1. Use only company device
2. Provide “Premium Laptop” for customer visit role (Corp lending, MarCom, …)

Own device:

1. Allow for ”Multi-company working” employee
2. Need register
3. Required EMS E3
4. Not allow for Sensitive data access employee
5. Show up the device with IT for a verification when leave

Mobile/Tablet

1. Need EMS E3 for all

Legal comply Checklist

การจัดทำ Checklist ตามการดำเนินการให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นเครื่องมือสำคัญที่จะช่วยให้องค์กรสามารถลำดับความสำคัญได้ว่าควรเร่งดำเนินการในข้อใด และสามารถเห็นภาพรวมของการดำเนินงานเป็นไปตามที่ พ.ร.บ. กำหนดไว้แล้วแค่ไหน

ตัวอย่าง การทำ Checklist

หัวข้อ	มาตรา	รายละเอียด/หน้าที่ของ Data Controller	สิ่งที่ต้องจัดเตรียม/ดำเนินการ	การดำเนินการของ
1.	19 ว.1 (บททั่วไป)	ผู้ควบคุมข้อมูล ต้อง 1. มี Lawful Basis ในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ("ประมวลผลข้อมูล") โดยหากไม่สามารถอ้าง Lawful Basis อื่นใดได้ ก็จะต้องขอ Consent ก่อนหรือขณะประมวลผลข้อมูล 2. ระบุ Lawful Basis ใน Privacy Notice ให้ชัดเจน จากการสำรวจข้อมูลและวัตถุประสงค์ในการประมวลผลข้อมูลจะขอ Consent ในกรณีดังต่อไปนี้ 1. ลูกค้า: การเสนอขายผลิตภัณฑ์ที่ไม่ใกล้เคียงกับผลิตภัณฑ์เดิมที่ลูกค้ามีอยู่, การทำ Profiling, การทำ Consolidated Statement, การขอใช้ Biometrics เพื่อการพิสูจน์และยืนยันตัวตนผ่าน NDID 2. พนักงาน (รวมถึงลูกจ้าง OA): การประมวลผลข้อมูล sensitive data เช่น ข้อมูล Biometrics เพื่อเข้าตึก และข้อมูลศาสนา เชื้อชาติ หมู่โลหิต ข้อมูลความพิการ ข้อมูลสุขภาพ ประวัติอาชญากรรม 3. ผู้รับการสัมภาษณ์ลงนิตยสาร	1. Consent ลูกค้า (Application form, Onboarding app)	- เตรียมร่าง Consent เรียบร้อยและได้ Review Final version แล้ว - จะประกาศให้แต่ละ BU เริ่มใช้พร้อมกันในช่วง [Q1/2021] - ระบบ Consent Management เริ่มใช้งาน [Tentative Q1/2021]
			2. Candidate Consent และ Onboard Consent	- Consent Final - Candidate Consent เริ่มใช้กับการสมัครงานตั้งแต่วันที่ [1 ตุลาคม 2563] To check with HR - Onboard Consent เริ่มใช้กับพนักงานใหม่ตั้งแต่วันที่ [1 ตุลาคม 2563] To check with HR - Employee Consent สำหรับพนักงานปัจจุบัน เริ่มใช้ตั้งแต่วันที่ [April 2021] To check with HR
			3. Consent ผู้รับการสัมภาษณ์ฯ	- Consent Final - เริ่มใช้ตั้งแต่วันที่ [•] รอสอบถามฝ่ายที่เกี่ยวข้อง]
			4. Privacy Notice	- โปรดดูรายละเอียดการดำเนินการตาม หัวข้อ 13. (มาตรา 23)

Awareness การสร้างความตระหนักรู้ถึงความสำคัญของข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ยังมีหน้าที่สำคัญในการทำ Awareness สร้างความรับรู้ให้กับพนักงานในองค์กรเพื่อให้มีความตระหนัก รู้ถึงความสำคัญของข้อมูลส่วนบุคคล เข้าใจในความเสี่ยงและผลกระทบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีผลกระทบกับองค์กร ซึ่งเป็นปัจจัยสำคัญในการขับเคลื่อนให้องค์กรสามารถดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้สำเร็จ

ตัวอย่าง การสร้าง Awareness

Training Class

กำหนดให้เป็นหลักสูตรที่เป็น Default Course ให้กับพนักงานทุกคน รวมถึงพนักงานใหม่

Infographic

สร้างสรรค์สื่อที่มีสีสัน เน้นรูปภาพในการนำเสนอ (One Page) และสรุปสาระสำคัญ เช่น Do / Don't เพื่อให้เข้าถึงได้ง่าย น่าสนใจ และสร้างการจดจำ

E-Learning

จัดทำสื่อการเรียนการสอนโดยเลือกหัวข้อที่สำคัญ หรือมีคำถามเข้ามาบ่อยๆ เพื่อให้พนักงานสามารถเลือกหัวข้อที่ตรงกับความสนใจ และสามารถเข้ามาฟังได้ด้วยตนเอง

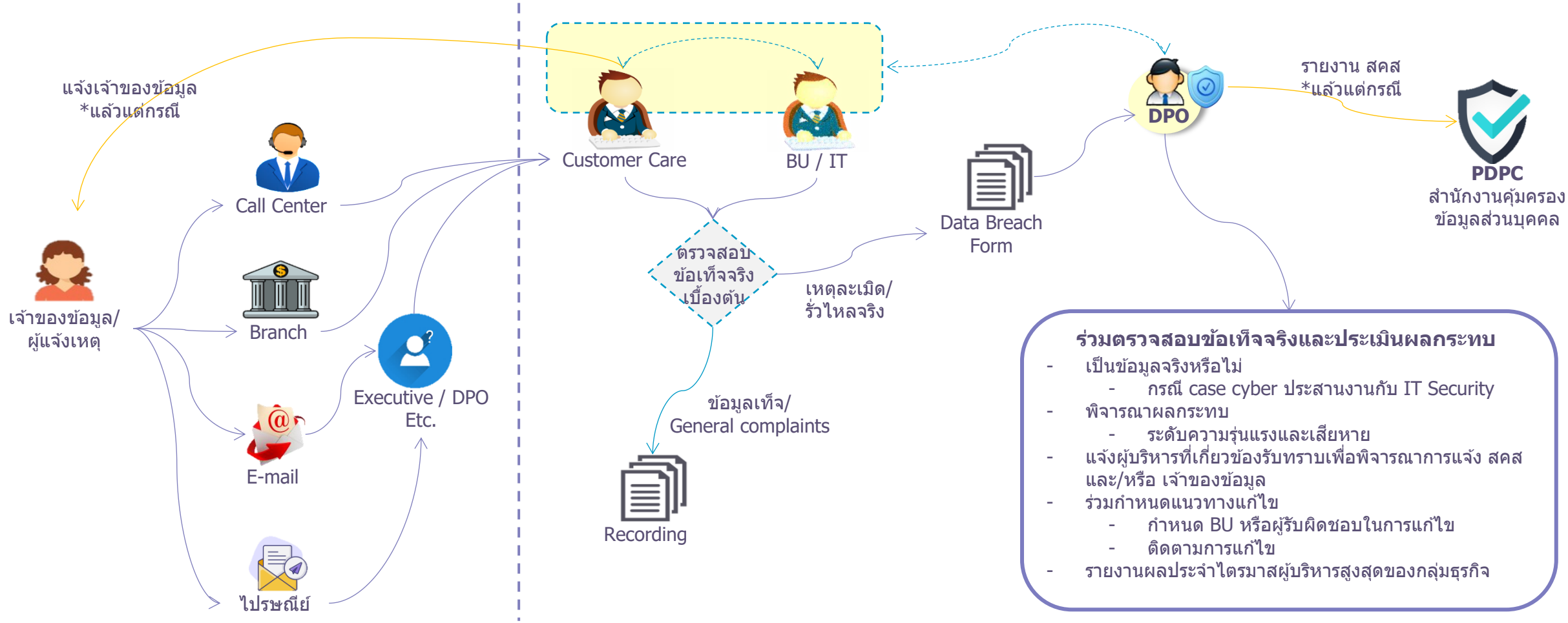
FAQ

รวมรวมคำถามและการให้ความเห็น จัดทำเป็น FAQ ส่งให้กับหน่วยงาน หรือว่างในรูปแบบ File FAQ ให้ผู้ปฏิบัติงานสามารถเข้าไปค้นหาได้ง่าย

Data Breach / Data Leaks Process กระบวนการจัดการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

เหตุละเมิดข้อมูลส่วนบุคคล

- การรั่วไหลหรือละเมิดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ส่งผลต่อข้อมูลส่วนบุคคลทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต



ร่วมตรวจสอบข้อเท็จจริงและประเมินผลกระทบ

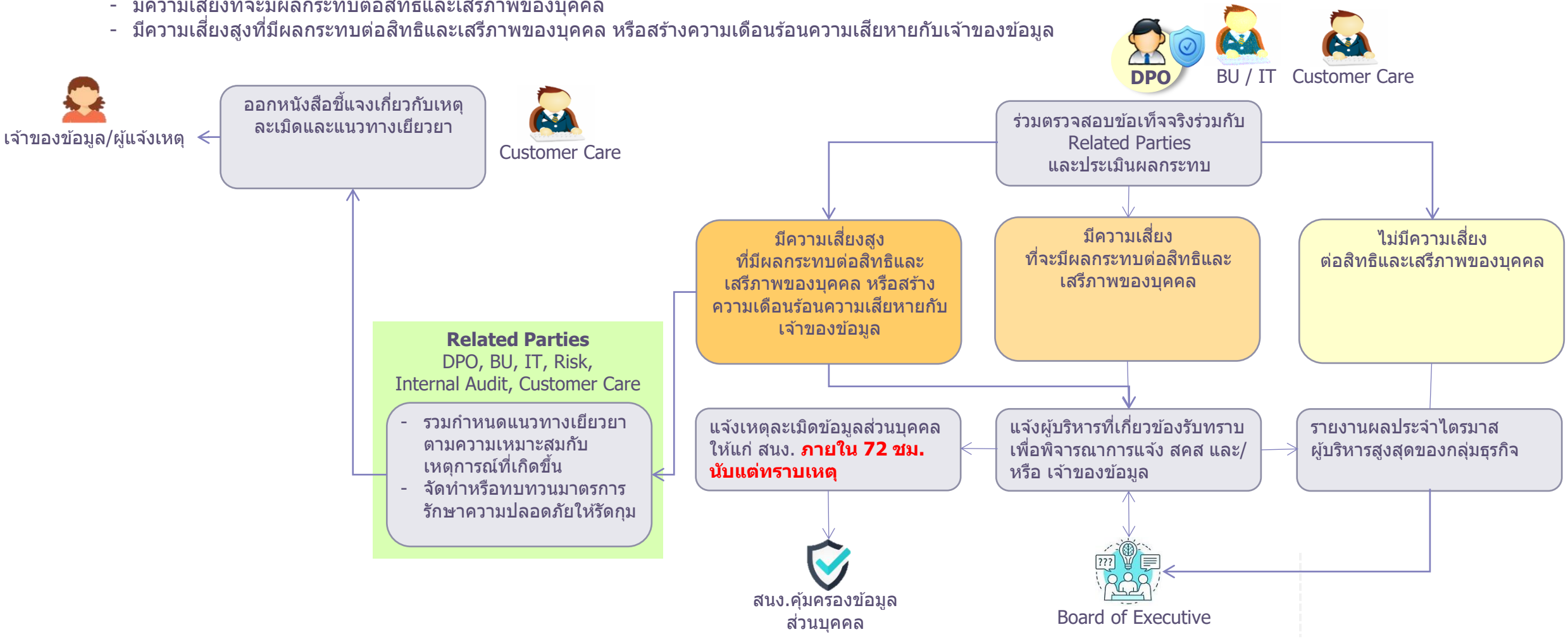
- เป็นข้อมูลจริงหรือไม่
  - กรณี case cyber ประสานงานกับ IT Security
- พิจารณาผลกระทบ
  - ระดับความรุนแรงและเสียหาย
- แจ้งผู้บริหารที่เกี่ยวข้องรับทราบเพื่อพิจารณาการแจ้ง สคส และ/หรือ เจ้าของข้อมูล
- ร่วมกำหนดแนวทางแก้ไข
  - กำหนด BU หรือผู้รับผิดชอบในการแก้ไข
  - ติดตามการแก้ไข
- รายงานผลประจำไตรมาสผู้บริหารสูงสุดของกลุ่มธุรกิจ

KIATNAKIN PHATRA

Data Breach / Data Leaks Process การจัดการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

<u>การการแจ้งเหตุละเมิดตามการพิจารณาผลกระทบและระดับความรุ่นแรง</u>

- พิจารณาเหตุการณ์ว่าเป็นเหตุละเมิดข้อมูลส่วนบุคคลหรือไม่
- พิจารณาผลกระทบตามระดับความรุ่นแรง
  - ไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล
  - มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
  - มีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือสร้างความเดือนร้อนความเสียหายกับเจ้าของข้อมูล



KIATNAKIN PHATRA

Example: Data Subject Right กระบวนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง กระบวนการขอใช้สิทธิ: ถอนความยินยอม ผ่านช่องทางสาขา

	Maintenance Form	Source System	Consent Management
 Customer	1 แจ้งขอถอนความยินยอม	2 - กรอกความประสงค์ในแบบฟอร์ม	
 Branch	3 - พิสูจน์ตัวตนลูกค้า	4 - ค้นหาข้อมูลลูกค้าและตรวจสอบว่าลูกค้าให้ความยินยอมนั้นไว้หรือไม่	4 - ค้นหาข้อมูลลูกค้าและตรวจสอบว่าลูกค้าให้ความยินยอมนั้นไว้หรือไม่
	5 - แจ้งผลกระทบจากการถอนความยินยอม		6 - บันทึกถอนความยินยอมผ่านระบบงาน
 Authorize			7 - ตรวจสอบและอนุมัติรายการ

Example: Data Subject Right กระบวนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง กระบวนการขอใช้สิทธิ: การขอใช้สิทธิอื่นๆ ผ่านช่องทางสาขา

	Request Form	Consent Management	Office365
 Customer	1 แจ้งขอใช้สิทธิ	2 - กรอกความประสงค์ในแบบฟอร์ม	
 Branch / Authorize	3 - ตรวจสอบเอกสารแสดงตนและพิสูจน์ตัวตนลูกค้า	4 - บันทึกรายการขอใช้สิทธิ - ผู้อนุมัติตรวจสอบและอนุมัติรายการ	
 Operation / Center	5 - ตรวจสอบข้อมูลลูกค้าเพิ่มเติมตาม Source System ที่จัดทำไว้ตาม Data Inventory	8 - บันทึกผลพิจารณาตามความเห็น PDPA Team - อนุมัติ, ปฏิเสธ 9 - ดำเนินการแจ้งผลการดำเนินการตามคำขอใช้สิทธิให้กับผู้ขอใช้สิทธิ	6 - ส่ง Mail แจ้งให้ PDPA Team และ Group Member PDPA พิจารณาผลกระทบร่วมกัน พร้อม Link Info.
			 PDPA Team 7 - พิจารณาการขอใช้สิทธิ - แจ้งผลการพิจารณากลับโดย Reply All - กรณีปฏิเสธให้แจ้งเหตุปฏิเสธกลับด้วย

SLA ดำเนินการแล้วเสร็จภายใน 30 วันนับจากวันที่ได้รับแจ้ง หรือตามที่กฎหมายจะประกาศกำหนดขึ้นภายหลัง

Data Controller & Data Processor : Open Issues

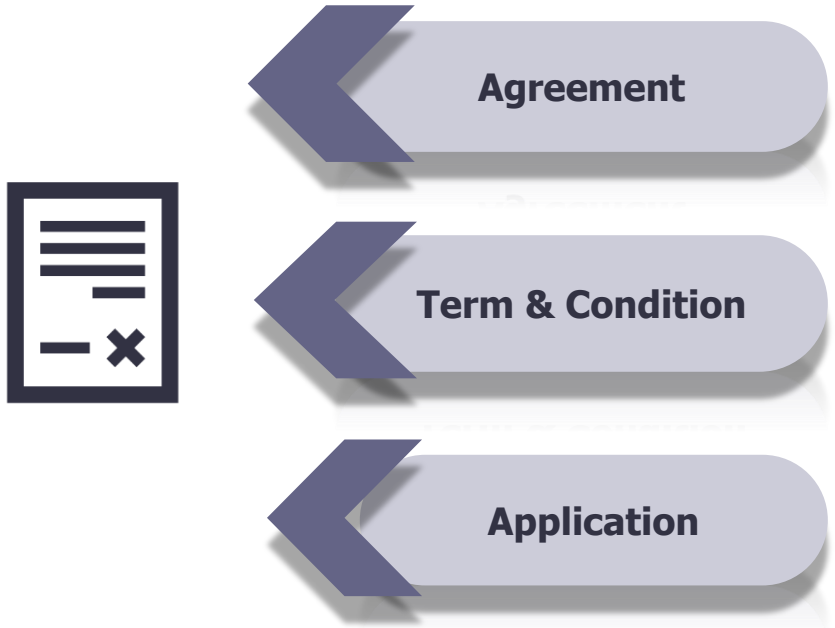
ไม่สามารถแยกได้ว่าใครเป็น Data Controller or Data Processor ?

ไม่มี Standard Template Agreement ที่ยอมรับในทุก Industry

คู่สัญญาอาจไม่ยอมลงนามใน Agreement โดยเฉพาะคู่สัญญาในต่างประเทศ

Data Controller & Data Processor : Legal Document

Legal Document : Type



Partner/Vendor/ Outsource

- สัญญา NDA
- สัญญาความร่วมมือ
- สัญญาจ้าง
- Privacy Notice

Prospect

เอกสารสำหรับกรอกข้อมูลส่วนบุคคลเพื่อ Drop Lead/สำรวจความพึงพอใจ Privacy Notice

Client

- Term and Condition
- Application
- Privacy Notice

Employee/ Candidate

- สัญญาจ้าง
- Application สมัครงาน
- Privacy Notice

KIATNAKIN PHATRA

Data Controller & Data Processor : Agreement

ข้อกำหนดที่ควรระบุไว้ในสัญญา

- คู่สัญญาต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือ อาจกำหนดหน้าที่ตามกฎหมายลงไปก็ได้ (เช่น หน้าที่ของ Data Processor)
- กำหนดหน้าที่เพิ่มเติมนอกเหนือจากที่ PDPA กำหนด แต่เกี่ยวเนื่องกับ PDPA เช่น 1) กำหนดกรอบระยะเวลาในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลของ Data Processor เนื่องจากกฎหมายไม่ได้กำหนดระยะเวลาที่แน่นอน 2) ระบุ SLA เพิ่มเติมจากหน้าที่ที่กฎหมายกำหนด
- กรณีเป็น Joint Controller จะต้องกำหนดขอบเขตหน้าที่ของแต่ละฝ่ายให้ชัดเจน และอาจกำหนด **Point of contact** สำหรับให้เจ้าของข้อมูลมาใช้สิทธิต่าง ๆ ตามกฎหมาย รวมถึงการให้ความร่วมมือในการดำเนินการตามตามสิทธิของเจ้าของข้อมูล เช่น กรณีเจ้าของข้อมูลใช้สิทธิลบ หรือทำลายข้อมูล หากเป็นข้อมูลที่ได้เปิดเผยต่อสาธารณะแล้ว ผู้ควบคุมข้อมูลอื่นก็จะต้องดำเนินการตามคำขอดังกล่าวด้วย
- ไม่ควรมีการจำกัดความรับผิด เนื่องจากจะทำให้ไม่สามารถไล่เบี้ยได้เต็มจำนวน
- การกำหนดให้ข้อสัญญาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลยังคงมีผล แม้สัญญาได้สิ้นสุดลงไปแล้ว
- การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อเลิกสัญญา

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

สาระสำคัญเรื่องการโอนข้อมูลส่วนบุคคลไปต่างประเทศ

- เป็นการโอนข้อมูลส่วนบุคคลตามข้อบังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ไปยังต่างประเทศหรือไม่

- ประเทศปลายทางที่รับโอนข้อมูลส่วนบุคคล มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่
  - ถ้าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลนั้นได้
  - ถ้าประเทศปลายทางที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคลจะยังไม่สามารถโอนข้อมูลส่วนบุคคลนั้นได้ โดยต้องพิจารณาถึงข้อยกเว้นหรือพิจารณาการกำหนดสิทธิ กติการะหว่างกันเพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครอง

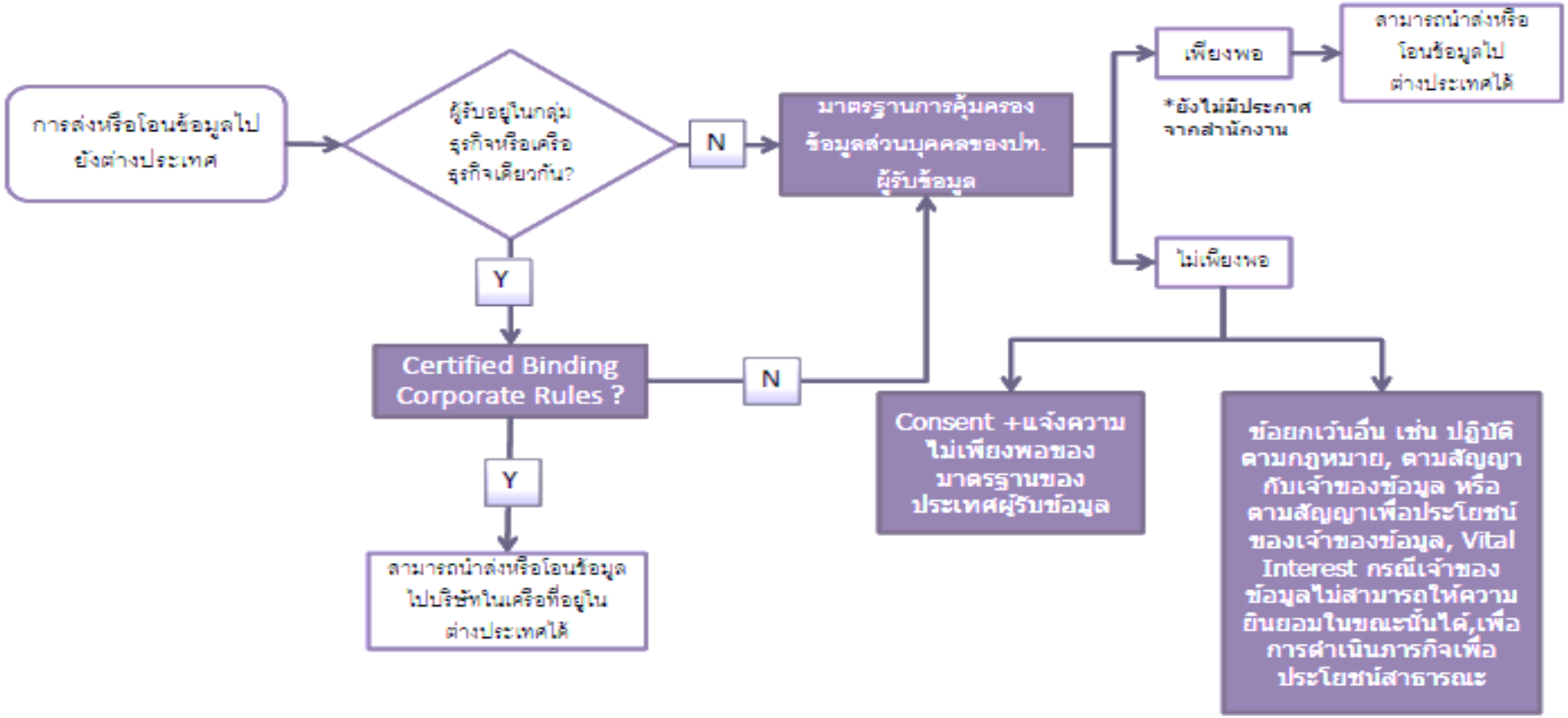
  กฎหมาย | องค์กร | พันธกรณีระหว่างประเทศ

- เป็นกรณีที่ได้รับการยกเว้นตามกฎหมายในการโอนข้อมูลส่วนบุคคลไปต่างประเทศปลายทางที่รับข้อมูลส่วนบุคคลที่ยังไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่

  กฎหมาย | ความยินยอม | สัญญา | Vital Interest | Legitimate Interest

- มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลการการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่ได้ตรวจสอบและรับรองจาก สนง.คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ



KIATNAKIN PHATRA

Document Template

Example: Document Template

Document	File
Data Discovery Template สำหรับตรวจสอบกิจกรรมให้เห็นถึงการเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคล	Data Discover
Data Inventory Template สำหรับสำรวจการจัดเก็บข้อมูลส่วนบุคคล ด้านรูปแบบของตัวข้อมูล สถานที่เก็บข้อมูล ระยะเวลาเก็บข้อมูล	Data Inventory Template
Self Assessment สำหรับให้แต่ละหน่วยงานใช้สอบทานตัวเองในกระบวนการสำคัญต่างๆ ที่มีข้อมูลส่วนบุคคล ว่าเป็นไปตามการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือไม่ เพื่อให้มีความพร้อมสำหรับการตรวจสอบจากหน่วยงานผู้ตรวจสอบ	Self Assessment
แบบฟอร์มการบันทึกเหตุการณ์ละเมิด รั่วไหลของข้อมูลส่วนบุคคล	Data Breach
การบันทึกเหตุการละเมิด รั่วไหลของข้อมูลส่วนบุคคล	Data Breach Record
การบันทึกการขอใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	Data Right Subject Record
การใช้สิทธิของเจ้าของข้อมูล ฐานกฎหมาย และเหตุปฏิเสธ ตารางการใช้สิทธิของเจ้าของข้อมูลแต่ละสิทธิอ้างอิงฐานกฎหมายใดบ้าง และมีเหตุปฏิเสธตามฐานกฎหมายข้อใดบ้าง	DataRightSubject Matrix

Appendix

ฐานการประมวลผลข้อมูล Lawful Basis

Research
เป็นการดำเนินการเพื่อจัดทำเอกสาร
ประวัติศาสตร์ จดหมายเหตุ
เพื่อการศึกษาหรือวิจัยหรือสถิติ

Vital interest
เพื่อป้องกันอันตรายต่อชีวิต ร่างกาย สุขภาพ

Legal Obligations
เป็นการดำเนินการเพื่อปฏิบัติตามกฎหมาย

Contractual Basis
เป็นการดำเนินการเพื่อปฏิบัติตามสัญญา
หรือตามคำร้องขอใช้บริการของเจ้าของ
ข้อมูลส่วนบุคคล

ฐานทางกฎหมาย
ของข้อมูลส่วนบุคคลทั่วไป
(Personal Data)

Legitimate interests
เพื่อประโยชน์โดยชอบด้วยกฎหมาย
ของผู้ควบคุมข้อมูลส่วนบุคคล

Public Task
ดำเนินการเพื่อภารกิจประโยชน์สาธารณะ

Consent
ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง

ฐานการประมวลผลข้อมูลอ่อนไหว Sensitive Data

01 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

02 เป็นการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรหรือสหภาพแรงงาน

03 เป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยความยินยอมโดยชัดแจ้งของเจ้าของ

04 เพื่อก่อตั้งสิทธิเรียกร้อง หรือการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมายหรือยกขึ้นต่อสู้ตามกฎหมาย

05 เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์
(สาธารณสุข แรงงาน ศึกษาวิจัย ประโยชน์สาธารณะ)

06 ได้รับความยินยอมโดยชัดแจ้ง(Explicit Consent)

ประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัว (Privacy Notice)

- ข้อมูลการเก็บรวบรวม ใช้หรือเปิดเผย ข้อมูลส่วนบุคคล และการจัดการข้อมูลส่วนบุคคล ซึ่งต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลให้ทราบ ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล

รายละเอียดประกาศความเป็นส่วนตัว (Privacy Notice)

1. วัตถุประสงค์และฐานทางกฎหมาย
2. ประเภทข้อมูลส่วนบุคคลและระยะเวลาเก็บข้อมูล
3. แหล่งที่มาของข้อมูล
4. ประเภทบุคคลที่ข้อมูลอาจถูกเปิดเผย
5. ข้อมูลและสถานที่ติดต่อ
6. สิทธิของเจ้าของข้อมูล

KIATNAKIN PHATRA

สิทธิของเจ้าของข้อมูลส่วนบุคคล Data Subject Right

สิทธิการขอถอนความยินยอม

- สามารถถอนความยินยอมได้ง่าย พอๆ กับตอนที่ให้ความยินยอม
- ไม่ได้รับผลกระทบจากการถอนความยินยอม
- ต้องยุติการประมวลผล

สิทธิขอเข้าถึงและขอรับสำเนาข้อมูล

สิทธิขอให้เปิดเผยการได้มาของข้อมูลที่ตนไม่ได้ให้ความยินยอม

สิทธิขอให้ส่งหรือโอนข้อมูลไปยัง ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น โดยวิธีการอัตโนมัติ

สิทธิขอรับข้อมูลที่มีการส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรง

สิทธิคัดค้านการประมวลผลข้อมูลที่ตนไม่ได้ให้ความยินยอม

สิทธิคัดค้านการประมวลผลเพื่อวัตถุประสงค์การตลาดแบบตรง

สิทธิขอให้ลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

- ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคลนั้นแล้ว
- ได้ถอนความยินยอม
- คัดค้านการประมวลผล
- ไม่มีฐานการประมวลผล
- ทำตามกฎหมาย

สิทธิระงับการประมวลผล

สิทธิขอให้ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

บทลงโทษ

ความรับผิดทางแพ่ง

- ผู้ควบคุมข้อมูล/ ผู้ประมวลผลข้อมูล กระทำการจงใจหรือประมาทเลินเล่อ จนก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนต่อเจ้าของข้อมูลส่วนบุคคล เว้นแต่
  (1) เหตุสุดวิสัย หรือ การกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลเอง
  (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ ที่มีอำนาจตามกฎหมาย

โทษทางอาญา

- ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูล Sensitive Data โดยไม่มี lawful basis หรือนอกเหนือจากวัตถุประสงค์ที่แจ้งไว้ หรือ ส่งข้อมูล Sensitive Data ไปต่างประเทศ โดยน่าจะทำให้เกิดการดูหมิ่นเกลียดชัง หรือเพื่อแสวงหาประโยชน์โดยมิชอบ
- กรรมการหรือผู้จัดการหรือบุคคลผู้รับผิดชอบในการดำเนินงานของนิติบุคคลนั้นต้องรับโทษในกรณีที่นิติบุคคลกระทำความผิดหากสั่งการ หรือมีหน้าที่ต้องสั่งการแต่ละเว้นไม่สั่งการ

โทษ: จำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 5 แสนบาทหรือทั้งจำทั้งปรับ หรือ จำคุกไม่เกิน 1 ปี ปรับ หรือ ไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับแล้วแต่กรณี

โทษทางปกครอง

- ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติหน้าที่ตามกฎหมายกำหนด
- คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งลงโทษปรับทางปกครอง

โทษ: ปรับไม่เกิน 5 แสน, 1 ล้าน, 3 ล้าน หรือ 5 ล้านบาท แล้วแต่กรณี

ตัวอย่างบทลงโทษ

เปิดเผยข้อมูลแก่ผู้อื่นโดยไม่ชอบด้วยกฎหมาย

- โทษอาญา
จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาทหรือทั้งจำทั้งปรับ
- โทษละเมิด

ส่งข้อมูลลูกค้าให้แก่พนักงานสถาบันการเงินอื่นเพื่อให้ติดต่อขายผลิตภัณฑ์ทางการเงิน

- โทษอาญา
จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
- โทษปกครอง
ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

ไม่แจ้ง Privacy Notice หรือไม่แจ้งผลกระทบจากการถอนความยินยอม

- โทษปกครอง
ปรับไม่เกิน 1 ล้านบาท

ขอ Consent จากเจ้าของข้อมูลไม่ถูกต้อง

- โทษอาญา
จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ หรือจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- โทษปกครอง
ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

ไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่กำหนด

- โทษปกครอง
ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

ตัวอย่างบทลงโทษ

ส่งข้อมูลเข้า Email หรือ Line ส่วนตัว และข้อมูลรั่วไหลไปภายนอก

- โทษปกครอง ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

Copy ข้อมูลลูกค้านำออกไปภายนอก เพื่อติดต่อเสนอขายผลิตภัณฑ์ทางการเงินของสถาบันการเงินอื่น

- โทษอาญา จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
- โทษปกครอง ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

เก็บข้อมูลกลุ่ม Prospect Customer จากแหล่งอื่น

- โทษปกครอง ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

ไม่ลบหรือทำลายข้อมูลเอกสารตามวิธีการหรือระยะเวลาที่กำหนด

- โทษปกครอง ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด

ไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัย

- โทษปกครอง ปรับไม่เกิน 3 ล้านบาท
- โทษละเมิด