# EP4: PDPA Readiness Speed-up

## Webinar series

# Previously… Key Takeaway

## PDPA Live Series EP1


- ความเสี่ยงของ PDPA ใกล้ตัวกว่าที่คิด ความเสี่ยงของการรั่วไหลของข้อมูล
- ความเสี่ยงและอุบัติการณ์ที่เกิดขึ้น ไม่ได้ขึ้นอยู่กับขนาดธุรกิจ
- หลักของการวางแผนจัดการ PDPA ที่ดี ต้องสอดคล้องกับกลยุทธ์ทางธุรกิจ

## Management Action EP2

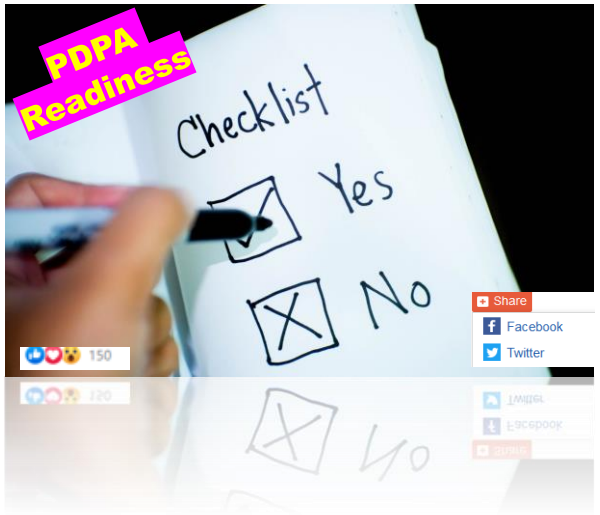

- ผู้บริหารมีความเข้าใจในหลักการปฏิบัติของกฎหมาย PDPA อย่างแท้จริง
- เราทราบประเภทของข้อมูลที่บริษัทเก็บอยู่ ว่าผลกระทบเชิงธุรกิจมาน้อยเพียงใด / เรามีแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลอย่างไร
- ผู้บริหารต้องทราบระดับ “ความพร้อม” ของบริษัท/องค์กร ในการรับมือในการปฏิบัติตามกฎหมาย PDPA

# Previously… Key Takeaway

## PDPA Person in Charge EP3


- เข้าใจบทบาท ตำแหน่งหน้าที่ของเจ้าหน้าที่ปกป้องข้อมูล หรือ DPO และตำแหน่งที่เกี่ยวข้องอื่น ๆ อาทิ Data Processor / Controller เป็นต้น
- เข้าใจการให้กรอบการทำงาน และความรับผิดชอบของเจ้าหน้าที่ที่ชัดเจน

## PDPA Readiness Speed-up EP4




- Checklist 3 ด้าน เพื่อเร่งความพร้อมขององค์กร
- เข้าใจกรอบการทำงานภาพใหญ่ เพื่อสามารถตัดสินใจ มอบหมายหน้าที่ และสั่งการเพื่อดำเนินการได้อย่างมีประสิทธิภาพ

EP #4

# PDPA Readiness Speed-Up

**ความท้าทาย:** บทบาทหน้าที่ที่เปลี่ยนไปของกรรมการบริษัท
(from ensuring compliance to driving performance)

**เป้าหมาย:** เข้าใจกรอบการทำงานภาพใหญ่ด้าน PDPA เพื่อให้สามารถตัดสินใจ มอบหมายหน้าที่ และสั่งการดำเนินการได้อย่างมีประสิทธิภาพ

**เครื่องมือ:** 3 Checklists for Immediate Action Plans

**Check#1:**
PDPA Governance

จัดตั้งโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล

**Check#2:**
Incident Management

จัดเตรียมแผนรับมือสถานการณ์

**Check#3:**
Procedures and IT System

ปรับกระบวนการและขอบเขตงานด้านดิจิทัล

EP #4

# Check#1: จัดตั้งโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล (1/2)

นโยบาย และกรอบปฏิบัติที่เป็น “รูปธรรม” ในลักษณะที่เป็น Top-down approach

- ✓ ภาพใหญ่สุด: เอกสารในระดับ “นโยบาย” หรือ “ข้อบังคับ” ระดับองค์กร
  - ✓ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Corporate Privacy Policy)
  - ✓ คำประกาศสิทธิ์ หรือคำประกาศขอบเขตของ “ความเป็นส่วนส่วนตัว” (Privacy Notice)
  - ✓ มีการจัดทำนโยบาย Data Retention Policy สำหรับพนักงานภายใน
  - ✓ เอกสารประกาศสิทธิ์ และหน้าที่ของ Stakeholders ที่เกี่ยวข้อง
    - ✓ อาทิ DPO / Controller / Processor

***Privacy Policy*** *– an internal statement that instructs employees on the collection and the use of the data and specified the rights of data subjects*

***Privacy Notice*** *– A statement made to a data subject which states how the organization collects, uses, retains and discloses personal information*

EP #4

# Check#1: จัดตั้งโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล (2/2)


**ปรับโครงสร้างองค์กร เสริมทัพด้วยทีม PDPA**

- ✓ สร้างทีมงาน PDPA ประกอบไปด้วย DPO | Data Controller | Data Processor | IT Security Officer
- ✓ กำหนดรูปแบบการรายงานขึ้นสู่บอร์ด (reporting lines) และรูปแบบการทำงานแบบ cross-functional
- ✓ ควรจะมี Internal audit ด้าน Risk & Compliance ที่ดูแลด้าน PDPA

**แผนการฝึกอบรมบุคลากรในองค์กร**

- ✓ พัฒนาและติดตามแหล่งองค์ความรู้ สร้างช่องทางติดต่อระหว่างองค์กรและแหล่งข้อมูล เช่น สคส.
- ✓ หน่วยฝึกอบรมมีการบรรจุความรู้ด้าน PDPA เป็นหนึ่งในหลักสูตรภาคบังคับของพนักงานทุกระดับ

**การจัดตั้งช่องทางสื่อสารประชาสัมพันธ์ด้านการป้องกันข้อมูลส่วนบุคคล**

- ✓ กำหนดช่องการการสื่อสาร และดำเนินการสื่อสารไปยังพนักงาน-เจ้าหน้าที่ทุกระดับชั้น
- ✓ สร้างวัฒนธรรมองค์กรที่พร้อมสำหรับการเคารพ การใช้ การเปิดเผยข้อมูลส่วนบุคคล
- ✓ สร้าง Hotline สายด่วนรายงานการละเมิด & FAQ (ทั้งภายในและภายนอก)

EP #4

# Check#2: จัดเตรียมแผนรับมือสถานการณ์ (incident management)


**แผนรับมือสถานการณ์**
**และความรับผิดชอบ (accountability)**

- ✓ เตรียมและอัพเดท แผนรับมือสถานการณ์ และแนวทางการตอบสนองต่อ incident ที่เกิดขึ้น
- ✓ ต้องระบุถึง PIC อย่างชัดเจน ห้ามกำหนดหรือมอบหมายแบบลอย ๆ
- ✓ Delegate ผู้รับผิดชอบในองค์กร ต้องระบุทั้ง “ตำแหน่ง” และ “ชื่อบุคคล”
- ✓ Risk & Compliance: PDPA’s spokesperson
- ✓ ซักซ้อมผ่านเหตุการณ์จำลอง (simulation test)

Criteria for assessing the severity of personal data breaches

- Data Processing Context (DPC) – main factor
- Ease of Identification (EI) – correcting factor
- Circumstances of Breach (CB) – adjustments

https://www.enisa.europa.eu/publications/dbn-severity

EP #4

# Check#3: ปรับกระบวนการ และขอบเขตงานด้านดิจิทัล (1/3)

**ปรับกระบวนการเพื่อ**
**การลดความเสี่ยงขององค์กร**

- ✓ เพิ่มหัวข้อ privacy compliance ให้เป็นส่วนหนึ่งของ audit framework
- ✓ สร้างความมั่นใจในกระบวนการที่มีการใช้ข้อมูลส่วนบุคคล ทั้งที่ใช้ภายใน และเชื่อมโยงกับภายนอก
  - ✓ Security diligence (integrity & confidentiality)
  - ✓ Purpose limitation / Storage limitation / Data minimization
  - ✓ Visibility of onwards data flows
- ✓ ทบทวนสัญญากับ service providers และ 3rd party
  - ✓ ปรับรูปแบบสัญญาให้ comply กับ PDPA
  - ✓ จัดทำรายการของสัญญาที่ต้องเปลี่ยน จัดอันดับความสำคัญ และแผนในการปรับเปลี่ยน
  - ✓ ความรับผิดชอบ (liability provisions) ในกรณีที่เกิดการรั่วไหล (breaches) จากคู่สัญญา
- ✓ ติดตามชุดข้อมูลที่ไหล เข้า-ออก นอกประเทศ และทบทวน data export mechanisms

EP #4

# Check#3: ปรับกระบวนการ และขอบเขตงานด้านดิจิทัล (2/3)

**กระบวนการที่เพิ่มขึ้น จัดการอย่างไร?**

- Overhead cost ที่สูงขึ้น
- ความเสี่ยง-ช่องโหว่ที่มากขึ้น
- การติดตามแก้ไขเอกสารจำนวนมาก ที่ต้องมีการอัพเดทบ่อยครั้ง

**เตรียมเอกสาร ที่ “จำเป็น” ให้พร้อมใช้งานเสมอ**

- ✓ เอกสาร (document) คือเครื่องมือหลักที่ใช้ในการกำหนดขั้นตอนการทำงาน (procedure)
- ✓ เพราะฉะนั้นองค์กรที่มีมาตรฐานการทำงาน เช่น ISO 27701 จะมีกระบวนการที่รองรับ PDPA
- ✓ จัดเตรียมเอกสารที่แสดงแบบพิมพ์เขียว ชุดข้อมูล ช่องทางการไหล จุดประสงค์ในการประมวลข้อมูล สถานที่จัดเก็บของข้อมูลส่วนบุคคลภายในองค์กร

**การจัดเตรียมเอกสารคำยินยอม (consent form)**

- ✓ ข้อตกลงในการ “ใช้” “บริหารจัดการ” และ “ประมวลผล” ข้อมูลส่วนบุคคล (ต้องได้รับการยอมรับ)
- ✓ แบบฟอร์มการขออนุญาตเพื่อให้คำยินยอม หรือ Consent form [ทั้งภายใน-ระหว่างแผนก ภายนอก]
- ✓ แบบฟอร์มการร้องขอให้เปิดเผย/แสดงผลข้อมูลส่วนบุคคล (Request form Data subject)
- ✓ แบบฟอร์มการร้องขอถอนความยินยอมข้อมูลส่วนบุคคล (Request form Data subject)
- ✓ แบบฟอร์มการแจ้งเตือน หรือการเปลี่ยนแปลงสิทธิ์ในการใช้/บริหารจัดการข้อมูลส่วนบุคคล

EP #4

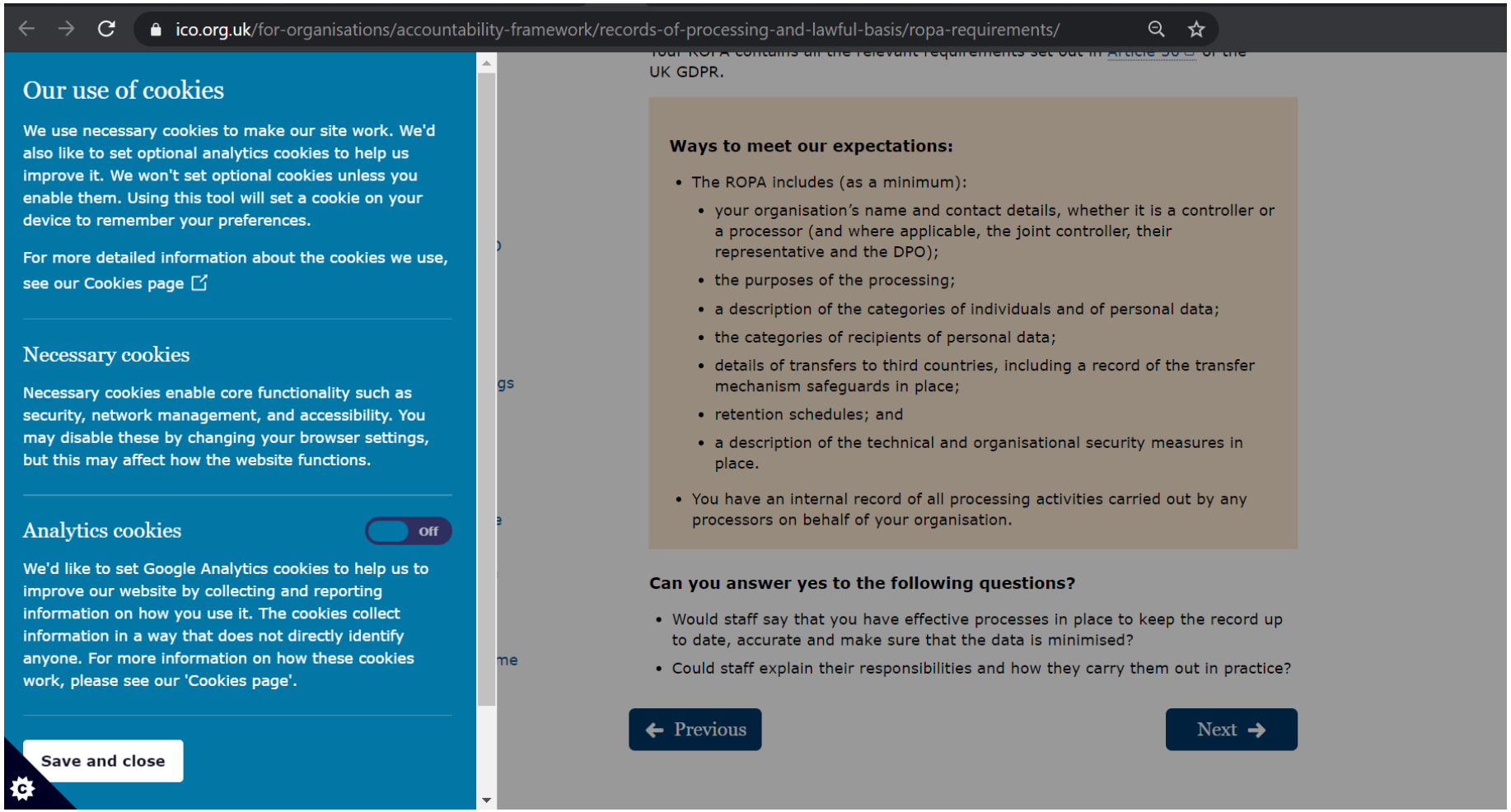
# Check#3: ปรับกระบวนการ และขอบเขตงานด้านดิจิทัล (3/3)

ทางออกคือการ implement ระบบดิจิทัล ที่ช่วยในการบริหารจัดการข้อมูลส่วนบุคคล

**ระบบดิจิทัล (privacy by design)**

- ✓ ระเบียนประวัติของข้อมูลส่วนบุคคลในระบบฐานข้อมูล
  - ✓ Digital Term & Condition with periodic acknowledgement
    - ✓ รองรับกระบวนการในกรณีที่มีการเปลี่ยนเนื้อหา consent & notification
    - ✓ รองรับการถอน consent ของ data subject ได้
    - ✓ รองรับ data retention management
    - ✓ รองรับสิทธิต่าง ๆ ของ data subject เช่น right to be forgotten, data portability, right to object
- ✓ กรณีที่มีช่องทางดิจิทัลระหว่างภายในและภายนอก: เช่น แสดงนโยบายการใช้ข้อมูลส่วนบุคคลผ่านทางคุกกี้ หรือโปรแกรมมิ่งสคริปต์ หรืออื่น ๆ
- ✓ แบบฟอร์ม Log เพื่อแสดงรายการและประวัติ รวมถึงกิจกรรมการแสดงผลข้อมูลส่วนบุคคล (ROPA)
  - ✓ จัดทำ data mapping exercise เป็นระยะ ๆ เพื่อให้ map up-to-date
  - ✓ จัดทำและคอยอัพเดทกระบวนการจัดเก็บ ROPA

# Cookie and Programming Script Example




https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

# ROPA Example

| | A | B | C | D | E | F | G | |
|---|---|---|---|---|---|---|---|---|
| 1 | Controller | | | | | | | |
| 2 | Name and contact details | | Data Protection Officer (if applicable) | | Representative (if applicable) | | | |
| 3 | **Name** | Example controller | **Name** | Example DPO | **Name** | N/A | | |
| 4 | **Address** | Street, city, postcode | **Address** | Street, city, postcode | **Address** | N/A | | |
| 5 | **Email** | Email address | **Email** | Email address | **Email** | N/A | | |
| 6 | **Telephone** | Tel. number | **Telephone** | Tel. number | **Telephone** | N/A | | |
| 7 | | | | | | | | |
| 8 | | | | | | Article 30 Record of Processing Activities | | |
| 9 | **Business function** | **Purpose of processing** | **Name and contact details of joint controller (if applicable)** | **Categories of individuals** | **Categories of personal data** | **Categories of recipients** | **Link to contract with processor** | **Names of third countries or internati organisations that personal data ar transferred to (if applicable)** |
| 10 | Finance | Payroll | N/A | Employees | Contact details | HMRC | N/A | N/A |
| 11 | Finance | Payroll | N/A | Employees | Bank details | HMRC | N/A | N/A |
| 12 | Finance | Payroll | N/A | Employees | Pension details | HMRC | N/A | N/A |
| 13 | Finance | Payroll | N/A | Employees | Tax details | HMRC | N/A | N/A |
| 14 | Human Resources | Personnel file | N/A | Employees | Contact details | N/A | N/A | N/A |
| 15 | Human Resources | Personnel file | N/A | Employees | Pay details | N/A | N/A | N/A |
| 16 | Human Resources | Personnel file | N/A | Employees | Annual leave details | N/A | N/A | N/A |
| 17 | Human Resources | Personnel file | N/A | Employees | Sick leave details | N/A | N/A | N/A |
| 18 | Human Resources | Personnel file | N/A | Employees | Performance details | N/A | N/A | N/A |
| 19 | Human Resources | Recruitment | N/A | Successful candidates | Contact details | Referee | N/A | N/A |
| 20 | Human Resources | Recruitment | N/A | Successful candidates | Qualifications | N/A | N/A | N/A |
| 21 | Human Resources | Recruitment | N/A | Successful candidates | Employment history | N/A | N/A | N/A |
| 22 | Human Resources | Recruitment | N/A | Successful candidates | Ethnicity | N/A | N/A | N/A |
| 23 | Human Resources | Recruitment | N/A | Successful candidates | Disability details | N/A | N/A | N/A |
| 24 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Contact details | N/A | N/A | N/A |
| 25 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Qualifications | N/A | N/A | N/A |
| 26 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Employment history | N/A | N/A | N/A |
| 27 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Ethnicity | N/A | N/A | N/A |
| 28 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Disability details | N/A | N/A | N/A |
| 29 | Sales | Direct marketing | N/A | Existing customers | Contact details | Processor - marketing co. | Link | N/A |
| 30 | Sales | Direct marketing | N/A | Existing customers | Purchase history | Processor - marketing co. | Link | N/A |

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

EP #3

# DISCUSSION

**Q&A**