

EP4: PDPA Readiness Speed-up

Webinar series

Previously... Key Takeaway

PDPA Live Series EP1



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

Management Action EP2



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

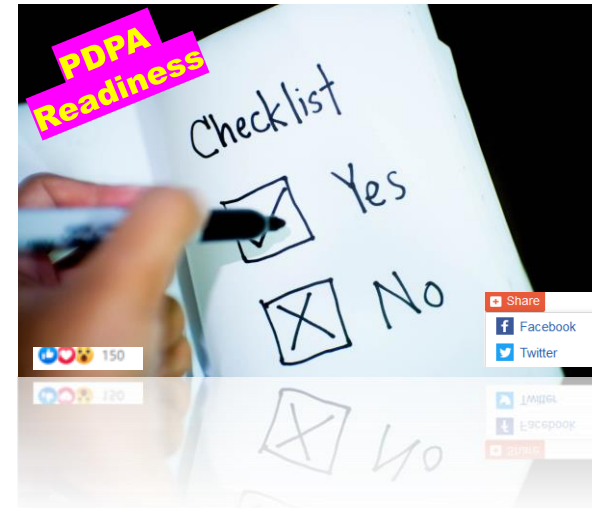
Previously... Key Takeaway

PDPA Person in Charge EP3



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

PDPA Readiness Speed-up EP4



- Checklist 3 ด้าน เพื่อเร่งความพร้อมขององค์กร
- เข้าใจรอบการทำงานภาพใหญ่ เพื่อสามารถตัดสินใจ มอบหมายหน้าที่ และสั่งการเพื่อดำเนินการได้อย่างมีประสิทธิภาพ

PDPA Readiness Speed-Up



ความท้าทาย: บทบาทหน้าที่ที่เปลี่ยนไปของกรมการบริษัท
(from ensuring compliance to driving performance)

เป้าหมาย: เข้าใจรอบการทำงานภาพใหญ่ด้าน PDPA เพื่อให้สามารถ
ตัดสินใจ มอบหมายหน้าที่ และสั่งการดำเนินการได้อย่างมีประสิทธิภาพ

เครื่องมือ: 3 Checklists for Immediate Action Plans

Check#1:

PDPA Governance

จัดตั้งโครงสร้างการกำกับ
ดูแลข้อมูลส่วนบุคคล

Check#2:

Incident Management

จัดเตรียมแผนรับมือ
สถานการณ์

Check#3:

Procedures and IT System

ปรับกระบวนการ
และขอบเขตงานด้านดิจิทัล

Check#1: จัดตั้งโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล (1/2)



นโยบาย และกรอบปฏิบัติที่เป็น “รูปธรรม” ในลักษณะที่เป็น Top-down approach

- ✓ ภาพใหญ่สุด: เอกสารในระดับ “นโยบาย” หรือ “ข้อบังคับ” ระดับองค์กร
 - ✓ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Corporate Privacy Policy)
 - ✓ คำประกาศสิทธิ หรือคำประกาศขอบเขตของ “ความเป็นส่วนส่วนตัว” (Privacy Notice)
 - ✓ มีการจัดทำนโยบาย Data Retention Policy สำหรับพนักงานภายใน
 - ✓ เอกสารประกาศสิทธิ 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

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**
- ✓ ควรมี **Internal audit** ด้าน Risk & Compliance ที่ดูแลด้าน PDPA

แผนการฝึกอบรมบุคลากรในองค์กร

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

การจัดตั้งช่องทางสื่อสารประชาสัมพันธ์ด้าน
การป้องกันข้อมูลส่วนบุคคล

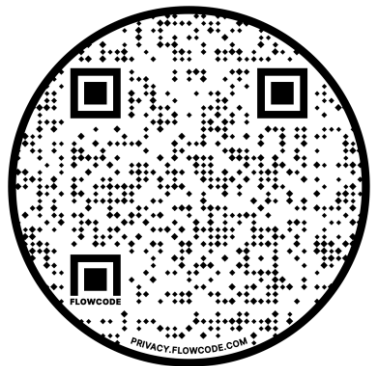
- ✓ กำหนด**ช่องทางการสื่อสาร** และดำเนินการสื่อสารไปยังพนักงาน-เจ้าหน้าที่ทุกระดับชั้น
- ✓ **สร้างวัฒนธรรมองค์กร**ที่พร้อมสำหรับการเคารพ การใช้ การเปิดเผยข้อมูลส่วนบุคคล
- ✓ สร้าง Hotline สายด่วนรายงานการละเมิด & FAQ (ทั้งภายในและภายนอก)

Check#2: จัดเตรียมแผนรับมือสถานการณ์ (incident management)



แผนรับมือสถานการณ์
และความรับผิดชอบ (accountability)

- ✓ เตรียมและอัปเดต 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

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
- ✓ ทบทวนสัญญาเกี่ยวกับ **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**

Check#3: ปรับกระบวนการ และขอบเขตงานด้านดิจิทัล (2/3)



เตรียมเอกสาร ที่ “จำเป็น” ให้พร้อมใช้งานเสมอ

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

การจัดเตรียมเอกสารคำยินยอม (consent form)

กระบวนการที่เพิ่มขึ้น จัดการอย่างไร?

- Overhead cost ที่สูงขึ้น
- ความเสี่ยง-ช่องโหว่ที่มากขึ้น
- การติดตามแก้ไขเอกสารจำนวนมาก ที่ต้องมีการอัปเดตบ่อยครั้ง

- ✓ 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 หรือการเปลี่ยนแปลงสิทธิในการใช้/บริหารจัดการข้อมูลส่วนบุคคล

Check#3: ปรับกระบวนการ และขอบเขตงานด้านดิจิทัล (3/3)

```

function(scope, element, attr, ngSwitchController) {
  // ...
  selectedTranscludes = attr.ngSwitch || attr.on,
  selectedElements = [],
  previousElements = [],
  selectedScopes = [];

  scope.$watch/watchExpr, function ngSwitchWatchAction(value) {
    // ...
    for (ii = 0, ii = previousElements.length; i < ii; ++i) {
      previousElements[i].remove();
    }
    previousElements.length = 0;

    for (ii = 0, ii = selectedScopes.length; i < ii; ++i) {
      var selected = selectedElements[i];
      selectedScopes[i].destroy();
      previousElements[i] = selected;
      animate.leave(selected, function() {
        previousElements.splice(i, 1);
      });
    }

    selectedElements.length = 0;
    selectedScopes.length = 0;

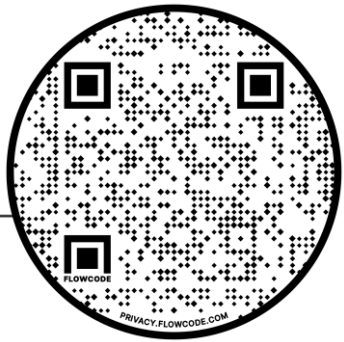
    if ((selectedTranscludes = ngSwitchController.cases["!" + value] || attr.ngSwitch)
        scope.$eval(attr.change);
    forEach(selectedTranscludes, function(selectedTransclude) {
      var selectedScope = scope.$new();
    });
  });
}

```

ทางออกคือการ implement ระบบดิจิทัล ที่ช่วยในการบริหารจัดการข้อมูลส่วนบุคคล

ระบบดิจิทัล (privacy by design)

- ✓ ระเบียบประวัติของข้อมูลส่วนบุคคลในระบบฐานข้อมูล
 - ✓ 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
 - ✓ จัดทำและคอยอัปเดตกระบวนการจัดเก็บ ROPA



Cookie and Programming Script Example

The screenshot shows a web browser window with the URL ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/ropa-requirements/. The page is titled "Our use of cookies" and contains a cookie consent banner. The banner is divided into three sections: "Our use of cookies", "Necessary cookies", and "Analytics cookies". The "Analytics cookies" section has a toggle switch set to "off". A "Save and close" button is visible in the bottom left corner of the banner. The main content of the page is titled "Ways to meet our expectations:" and lists several requirements for a Record of Processing Activities (ROPA). The requirements include: the ROPA includes (as a minimum): your organisation's name and contact details, the purposes of the processing, a description of the categories of individuals and of personal data, the categories of recipients of personal data, details of transfers to third countries, retention schedules, and a description of the technical and organisational security measures in place. Additionally, it states that you have an internal record of all processing activities carried out by any processors on behalf of your organisation. Below the requirements, there is a section titled "Can you answer yes to the following questions?" with two questions: "Would staff say that you have effective processes in place to keep the record up to date, accurate and make sure that the data is minimised?" and "Could staff explain their responsibilities and how they carry them out in practice?". Navigation buttons for "Previous" and "Next" are located at the bottom of the page.

Our use of cookies

We use necessary cookies to make our site work. We'd also like to set optional analytics cookies to help us improve it. We won't set optional cookies unless you enable them. Using this tool will set a cookie on your device to remember your preferences.

For more detailed information about the cookies we use, see our [Cookies page](#)

Necessary cookies

Necessary cookies enable core functionality such as security, network management, and accessibility. You may disable these by changing your browser settings, but this may affect how the website functions.

Analytics cookies off

We'd like to set Google Analytics cookies to help us to improve our website by collecting and reporting information on how you use it. The cookies collect information in a way that does not directly identify anyone. For more information on how these cookies work, please see our 'Cookies page'.

Save and close

Ways to meet our expectations:

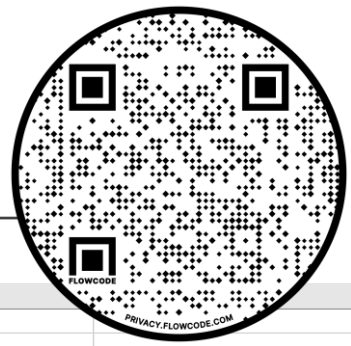
- The ROPA includes (as a minimum):
 - your organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
 - the purposes of the processing;
 - a description of the categories of individuals and of personal data;
 - the categories of recipients of personal data;
 - details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
 - retention schedules; and
 - a description of the technical and organisational security measures in place.
- You have an internal record of all processing activities carried out by any processors on behalf of your organisation.

Can you answer yes to the following questions?

- Would staff say that you have effective processes in place to keep the record up to date, accurate and make sure that the data is minimised?
- Could staff explain their responsibilities and how they carry them out in practice?

Previous Next

ROPA Example



Controller							
Name and contact details		Data Protection Officer (if applicable)		Representative (if applicable)			
Name	Example controller	Name	Example DPO	Name	N/A		
Address	Street, city, postcode	Address	Street, city, postcode	Address	N/A		
Email	Email address	Email	Email address	Email	N/A		
Telephone	Tel. number	Telephone	Tel. number	Telephone	N/A		
Article 30 Record of Processing Activities							
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 international organisations that personal data are transferred to (if applicable)
Finance	Payroll	N/A	Employees	Contact details	HMRC	N/A	N/A
Finance	Payroll	N/A	Employees	Bank details	HMRC	N/A	N/A
Finance	Payroll	N/A	Employees	Pension details	HMRC	N/A	N/A
Finance	Payroll	N/A	Employees	Tax details	HMRC	N/A	N/A
Human Resources	Personnel file	N/A	Employees	Contact details	N/A	N/A	N/A
Human Resources	Personnel file	N/A	Employees	Pay details	N/A	N/A	N/A
Human Resources	Personnel file	N/A	Employees	Annual leave details	N/A	N/A	N/A
Human Resources	Personnel file	N/A	Employees	Sick leave details	N/A	N/A	N/A
Human Resources	Personnel file	N/A	Employees	Performance details	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Contact details	Referee	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Qualifications	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Employment history	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Ethnicity	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Successful candidates	Disability details	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Contact details	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Qualifications	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Employment history	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Ethnicity	N/A	N/A	N/A
Human Resources	Recruitment	N/A	Unsuccessful candidates	Disability details	N/A	N/A	N/A
Sales	Direct marketing	N/A	Existing customers	Contact details	Processor - marketing co.	Link	N/A
Sales	Direct marketing	N/A	Existing customers	Purchase history	Processor - marketing co.	Link	N/A

DISCUSSION

Q&A