Personal Data Protection Act (PDPA)

พรบ. คุ้มครองข้อมูลส่วนบุคคล

9 Mar 2022

Agenda

1 

What is PDPA and PDPA Key Terms

2 

PDPA / Privacy Principles

3 

Data Subject Rights

4 

SCB Privacy Program and PDPA Checklist

WHAT IS THE PDPA?

The PDPA stands for **'The Personal Data Protection Act'**

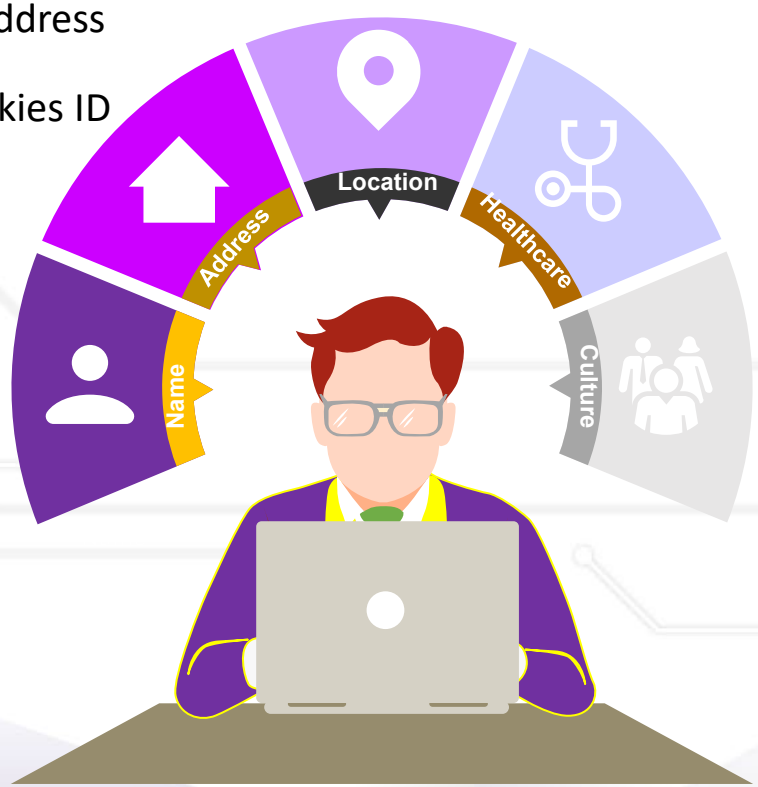
Applicable Law	Personal Data Protection Act B.E. 2562 (PDPA)
Effective	~~27 May 2020~~ → ~~1 Jun 2021~~ → **1 Jun 2022**
Scope	The collection, use, or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand
Penalties	Civil, criminal, and administrative liabilities
Breaches	Breach reporting within 72 hours

Personal Data and Sensitive Personal Data

Personal Data

Information relating to a living person, which directly or indirectly enables their identification. Sometimes is referred as personally identifiable information (PII).

Name	Birthday	IP address
E-mail	Home address	Cookies ID
Education	Employee ID	
Gender	Personal interest	
Occupation	Home zip code	
Photo	Phone number	



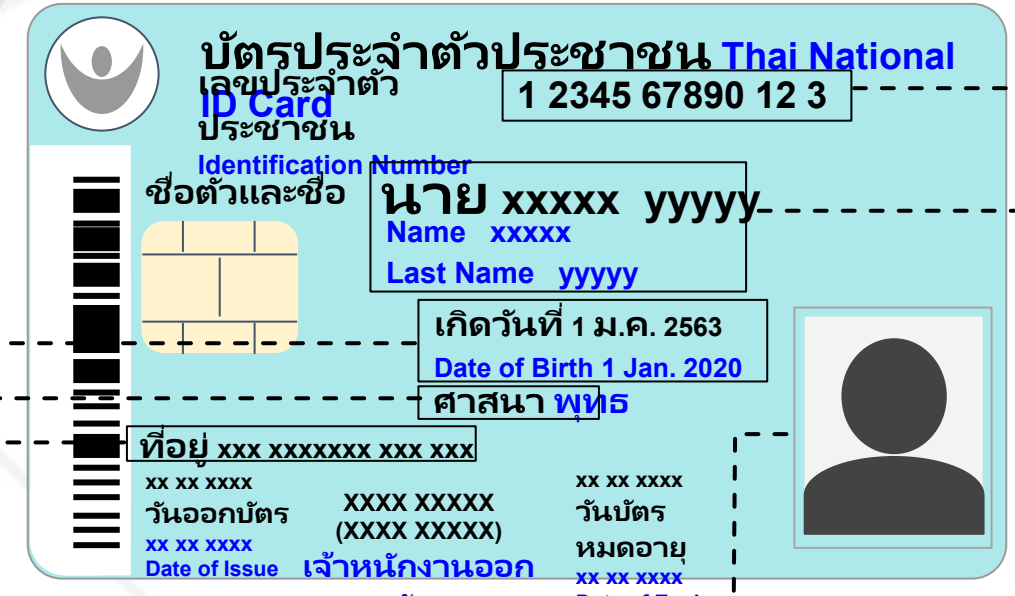
Sensitive Personal Data

Special category of personal data that is at risk of being unfairly used for discrimination.

- Medical or health conditions
- Genetic and biometric data
- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Sexual preference
- Information related to offences or criminal conviction

PERSONAL DATA AND SENSITIVE PERSONAL DATA

EXAMPLE



Identification number
Personal data

First name and last name
Personal data

Photo
Personal data

Address
Personal data

Religion
Sensitive personal data

Date of Birth
Personal data

PDPA Key Terms

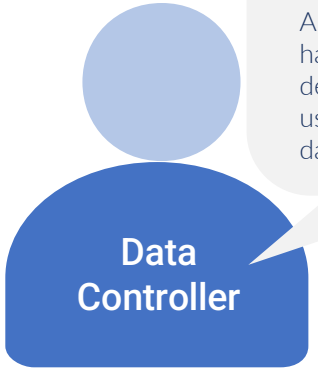
The person whose data is processed

Customers, Employees, Individual contractors, Board members, Prospect customers etc.

เจ้าของข้อมูลส่วนบุคคล

WHO decides WHY and HOW to process personal data

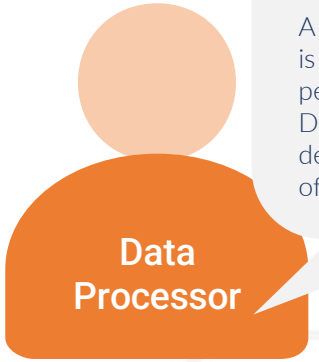
A person or a juristic person who has the power and duties to make decisions regarding the collection, use and/or disclosure of personal data



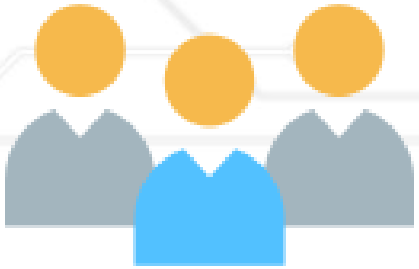
ผู้ควบคุมข้อมูลส่วนบุคคล

WHO processes personal data on behalf on Data Controller

A person or a juristic person who is responsible for processing of personal data on behalf of the Data Controller, BUT makes no decision on purposes and means of processing data



ผู้ประมวลผลข้อมูลส่วนบุคคล



คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

PDPA Key Terms (cont.)

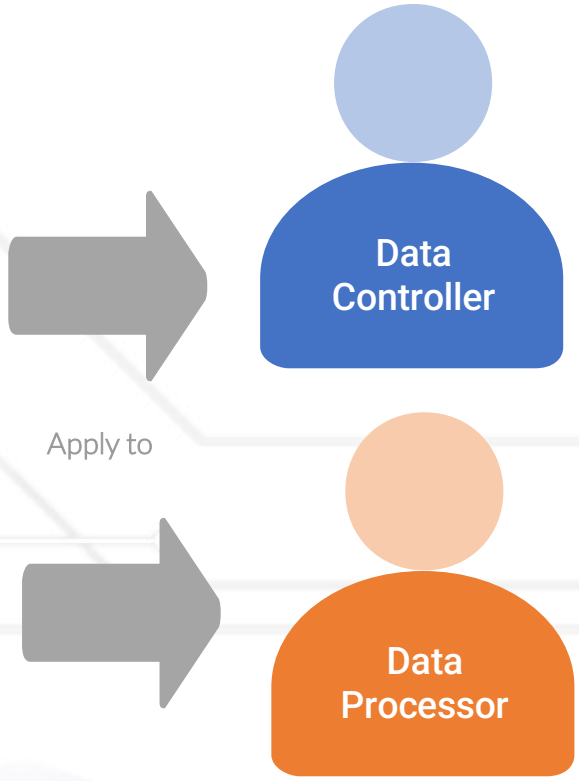
Data Protection Officer

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

A Data Protection Officer is required to be appointed by an organisation when:

- Organisation is a public authority or body
- Organisation's core activities require regular, systematic monitoring of individuals on a large scale
- Core activity of the organisation is the collection, use, or disclosure of the Personal Data

Apply to



DPO Responsibilities

- Give advice and recommendation with respect to compliance with the Act
- Verify and ensure data protection compliance within the organization
- Coordinate and cooperate with the regulators

Organization Responsibilities

- Not dismiss or terminate the DPO's employment by the reason that he/she performs his/her duties under the Act
- Able to directly report to the chief executive, if there is a problem when performing the duties
- Provide and support all necessary resources to carry out the DPO's tasks required of the role

The **Data Protection Officer** may be :-

- A staff of the Data Controller or the Data Processor

OR

- An external service provide under the contract with the Data Controller or the Data Processor

OR

- A single DPO designated under a group of undertakings

PDPA/PRIVACY PRINCIPLES

Lawfulness, Fairness, and Transparency

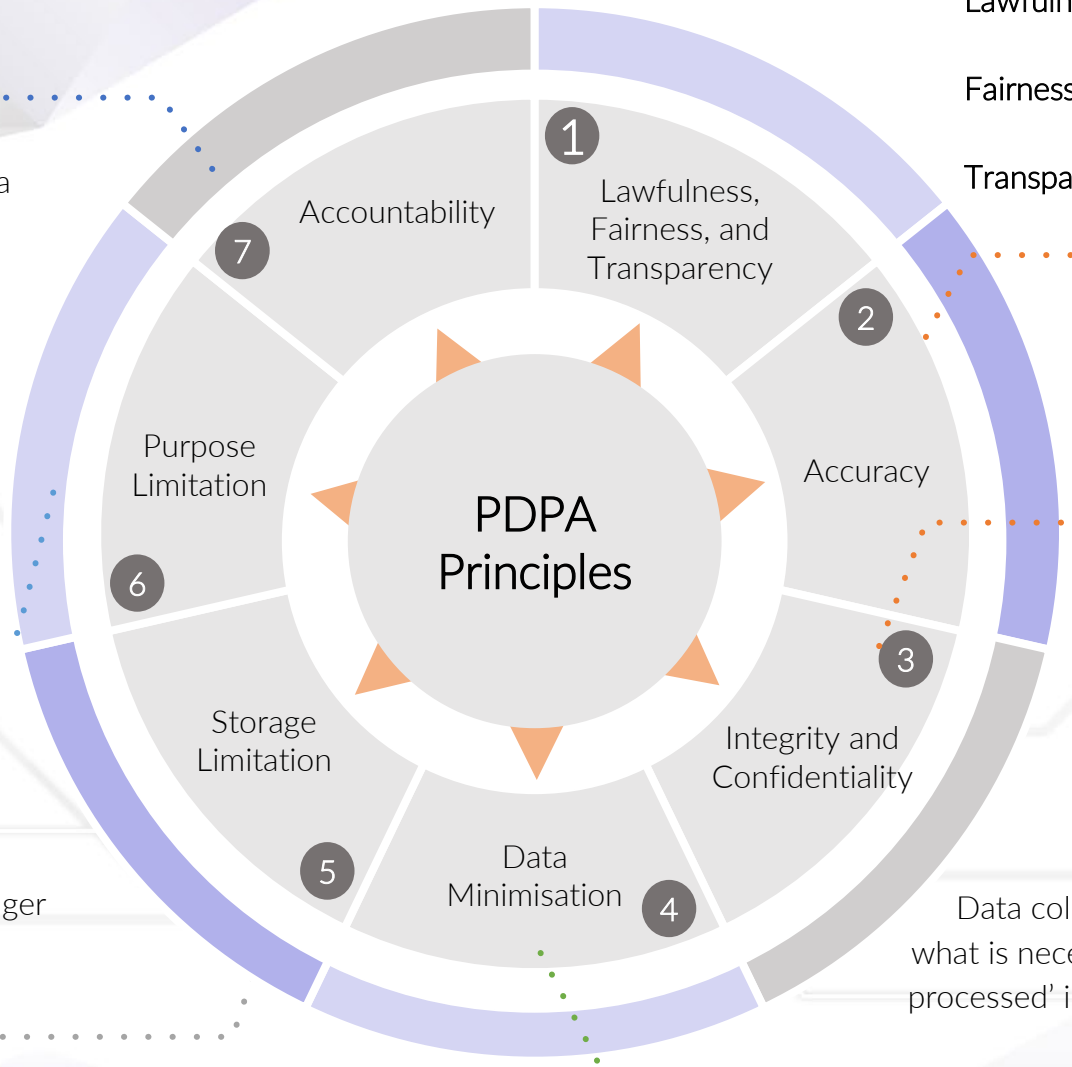
Lawfulness: Necessary in relation to lawful purpose of Data Controller

Fairness: Personal data must be processed in ways that people would reasonably expect

Transparency: Purpose is notified to data subject

Accountability

Data controllers and data processors are accountable for their processing of personal data and must demonstrate their compliance to all data protection principle



Accuracy

Personal data must be accurate and, where necessary, kept up to date

Purpose Limitation

Data can only be used, collected, and disclosed for specific processing purposes and no other, without further consent

Integrity and Confidentiality

Personal data must be processed in a manner that ensures appropriate security and protection

Storage Limitation

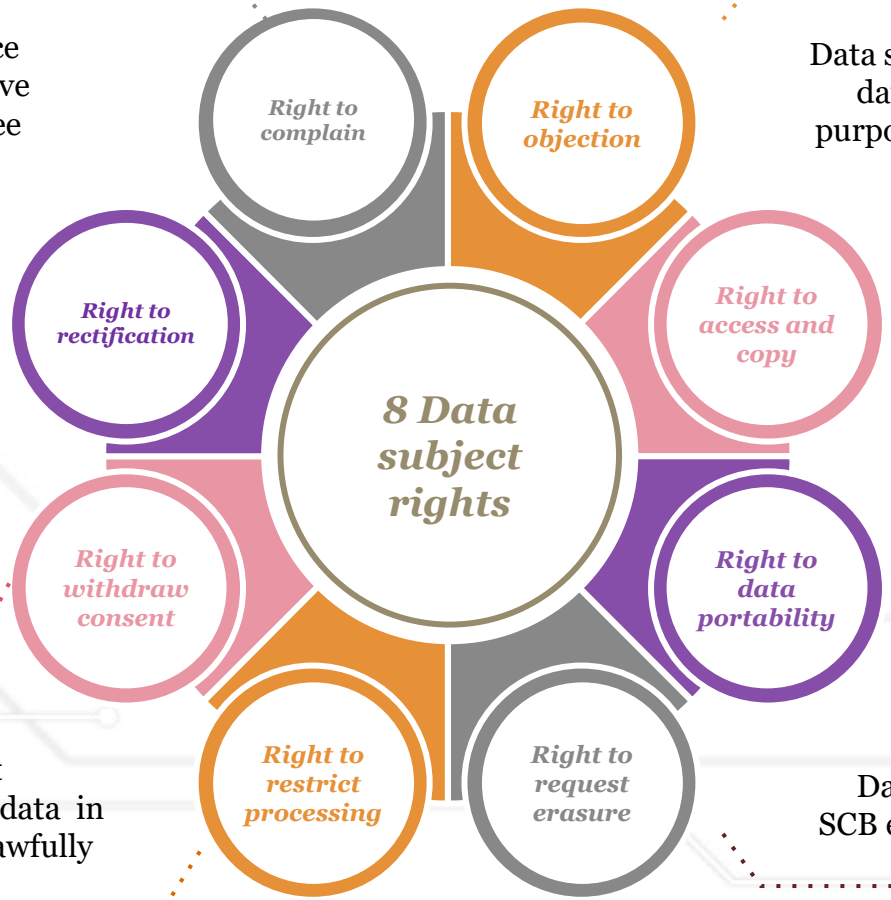
Personal data should be 'kept in a form which permits identification of data subjects for no longer than necessary' i.e. personal data is no longer required then it should be deleted

Data Minimisation

Data collected should be 'adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed' i.e. only collect the personal data which is limited to what is necessary for the purpose.

Data Subject Rights

8 Data Subject Rights



8. Right to complain

If Data Controller does not act in accordance with data subject requests, data subjects have the right to complain to an expert committee to order for the Bank to take such action.

7. Right to rectification

Data subjects have the right to request that SCB take actions to ensure that their personal data remains accurate, up-to-date, complete and not misleading.

6. Right to withdraw consent

Data subjects have the right to withdraw their consent given to SCB at any time.

5. Right to restrict processing

Data subjects have the right to request restricting the processing of personal data in case of certain conditions; e.g. it's unlawfully processed

1. Right to objection

Data subjects have the right to object to use of their data in circumstances where the data is used for purpose of marketing, or collected without consent

2. Right to access and copy

Data subjects have the right to request access to and obtain a copy of their personal data, which is under the responsibility of the Bank

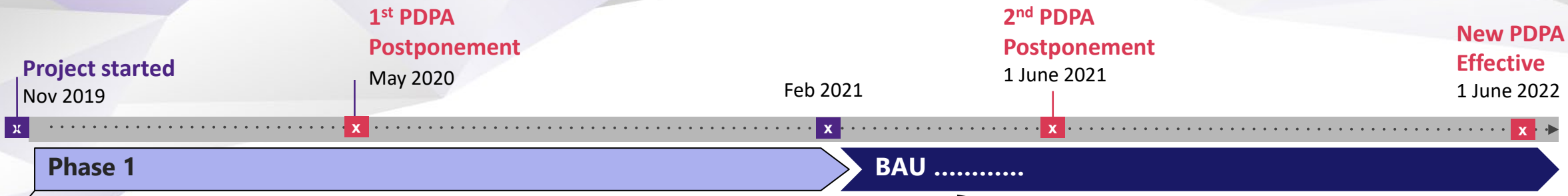
3. Right to data portability

Data subjects have the right to receive their personal data from SCB in a readable or commonly used format

4. Right to erasure

Data subjects have the right to request that SCB erases or anonymizes their personal data if the request matches certain guidelines

SCB PRIVACY PROGRAM



Ten privacy domains have been covered in the SCB Privacy Program for PDPA Readiness

1 Strategy & Governance

- Governance model
- Organization Structure
- Policies and regulations

2 Notice & Consent

- Privacy Notice
- Consent messages

3 Data Life Cycle

- Record of Processing (ROP) activities
- Data Governance & Classification

4 Privacy Impact Assessment

- Data Privacy Impact Assessment (DPIA)
- Privacy by Design

5 Data Subject Rights

- Processing of consents and data subject requests, such as access, deletion, objection

6 Information Security

- Information Security Controls and Standards

7 Privacy Incident Mgt.

- Data breach handling and responses, including notification regulators and data subjects

8 & 9 Third Party Mgt. and Cross-border Data Transfer

- Third Party management approach
- Safeguarding measures in the access and transfer data to Third parties
- Standard Contractual Clauses

10 Training & Awareness

- Training materials
  - Bank-wide
  - Role based
- Awareness program

PDPA Checklist

1 Tone from the Top

Board of Director, Audit Committee, Technology Committee are aware of PDPA implementation in the Bank

2 Privacy Policy / Privacy Notice

- Bank's Data Privacy and Protection Policy approved by Board of Director
- Privacy Notice – both customer and employee versions is published in Internet and Intranet websites

3 Consent

- Consents are identified and asked from data subjects prior to collecting, use and disclosure
- Marketing Consent, Cross-sell Consent, Sensitive data Consent, Cross-border data transfer consent , etc.

4 Record of Processing Activities

- Data Inventory Registration (DIR)
- Data Sharing / Data Ingestion Form
- Data Request Form

5 Data Subject Rights

- All processes are in place, the data subjects can exercise their rights through Branch and Call center.
- Withdrawal consent can be done through e-channels

6 Data Breach Notification

- Data Breach Management process
- Data Breach assessment template
- Data Breach Report template

7 Data Processing Agreement

- Standard Data Processing Agreements
- Third-party Inventory
- Third-party criticality assessment and Control checklist

8 Cross-border Data Transfer

- List of approved countries , waiting for PDPC announcement
- However, the Bank has announced in Privacy Notice for cloud services storage

9 Data Protection Officer

- Data Protection Officer was appointed, and Data Protection Office was established in Feb 2020

9 PDPA Checklist items listed above referred from "งานสัมมนาออนไลน์ ตรวจสอบความพร้อมให้มั่นใจก่อน PDPA มีผลบังคับใช้" โดย ผศ.ดร. ปิยะบุตร บุญอร่ามเรือง อาจารย์ประจำคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Appendix

Examples of Tone from the Top and Creating awareness

"ประชาชนผู้เป็นเจ้าของข้อมูลนั้น
มีสิทธิที่จะรับทราบได้ว่า
เราเก็บข้อมูลเขาไปทำอะไร
และเราจะไม่ทำอะไรกับข้อมูลเหล่านั้น
ในทางที่เราไม่ตกลงกับเขามาก่อน"

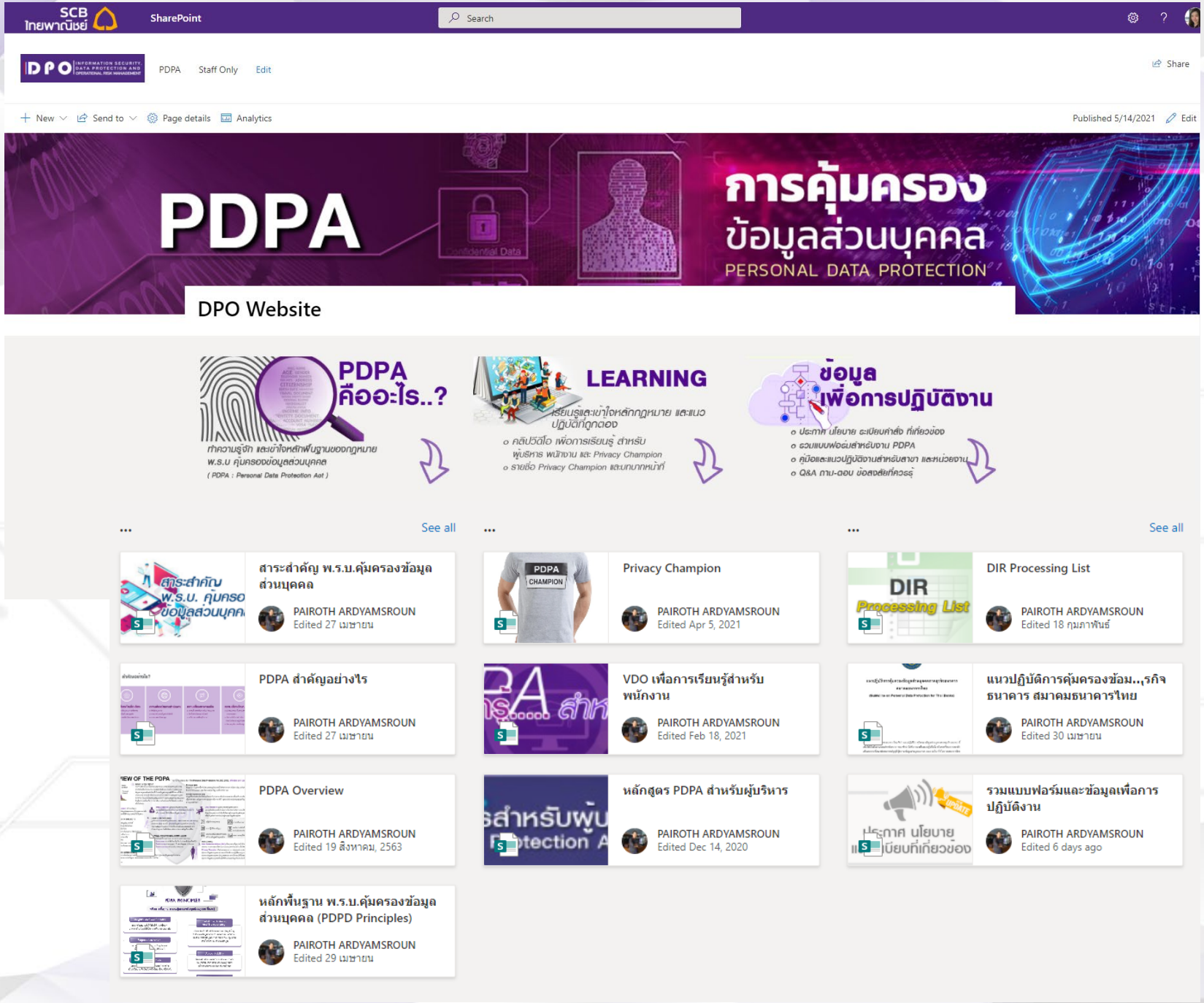
สำคัญที่สุดคือ วัฒนธรรมที่เกี่ยวข้องกับการดูแลข้อมูล
ไม่ให้ตกหล่นรั่วไหล หรือนำไปใช้ในทางที่ผิด

PDPA

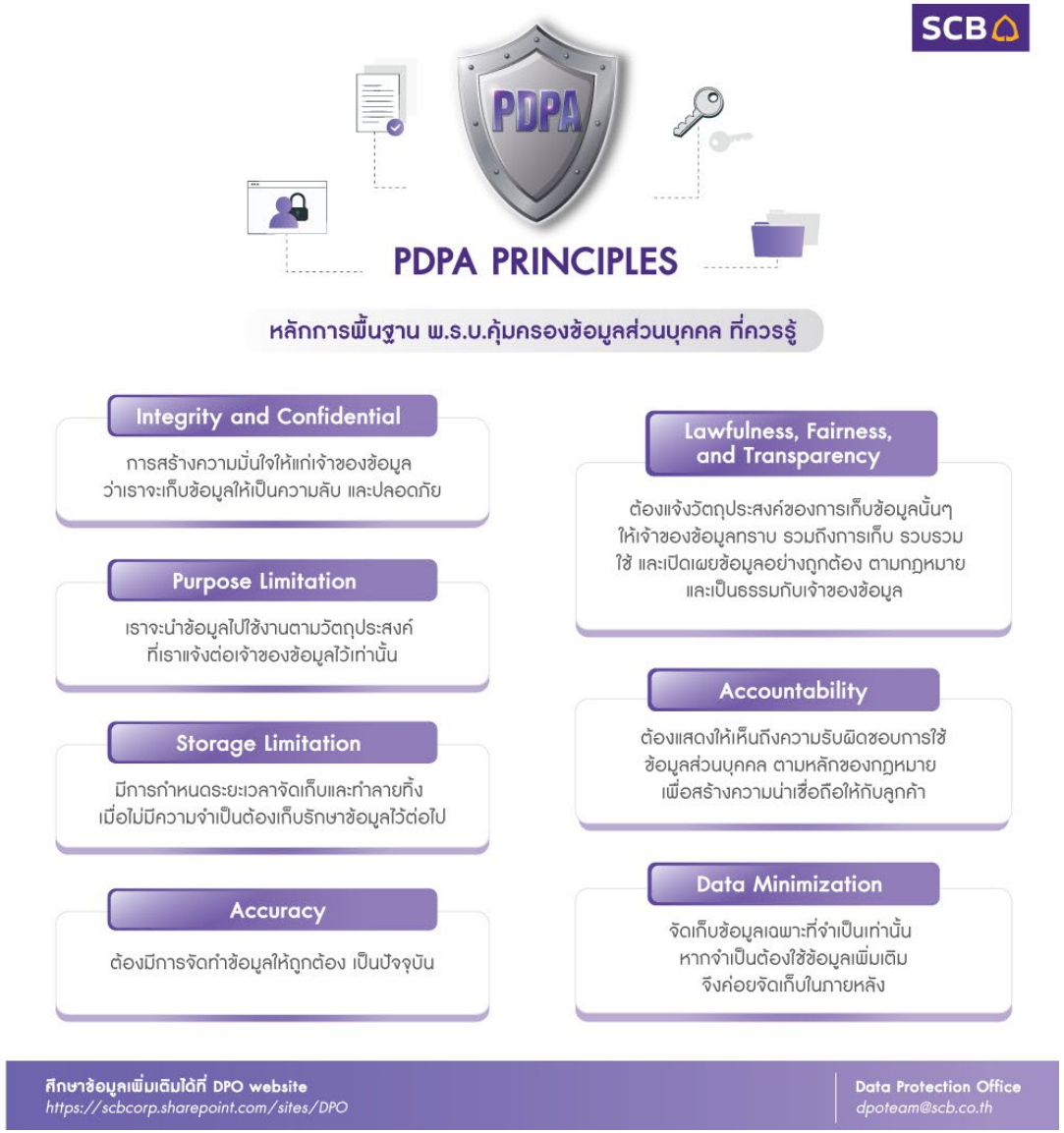
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ดร.ทวีศักดิ์ กออนันตกูล
กรรมการอิสระ
และประธานคณะกรรมการเทคโนโลยี

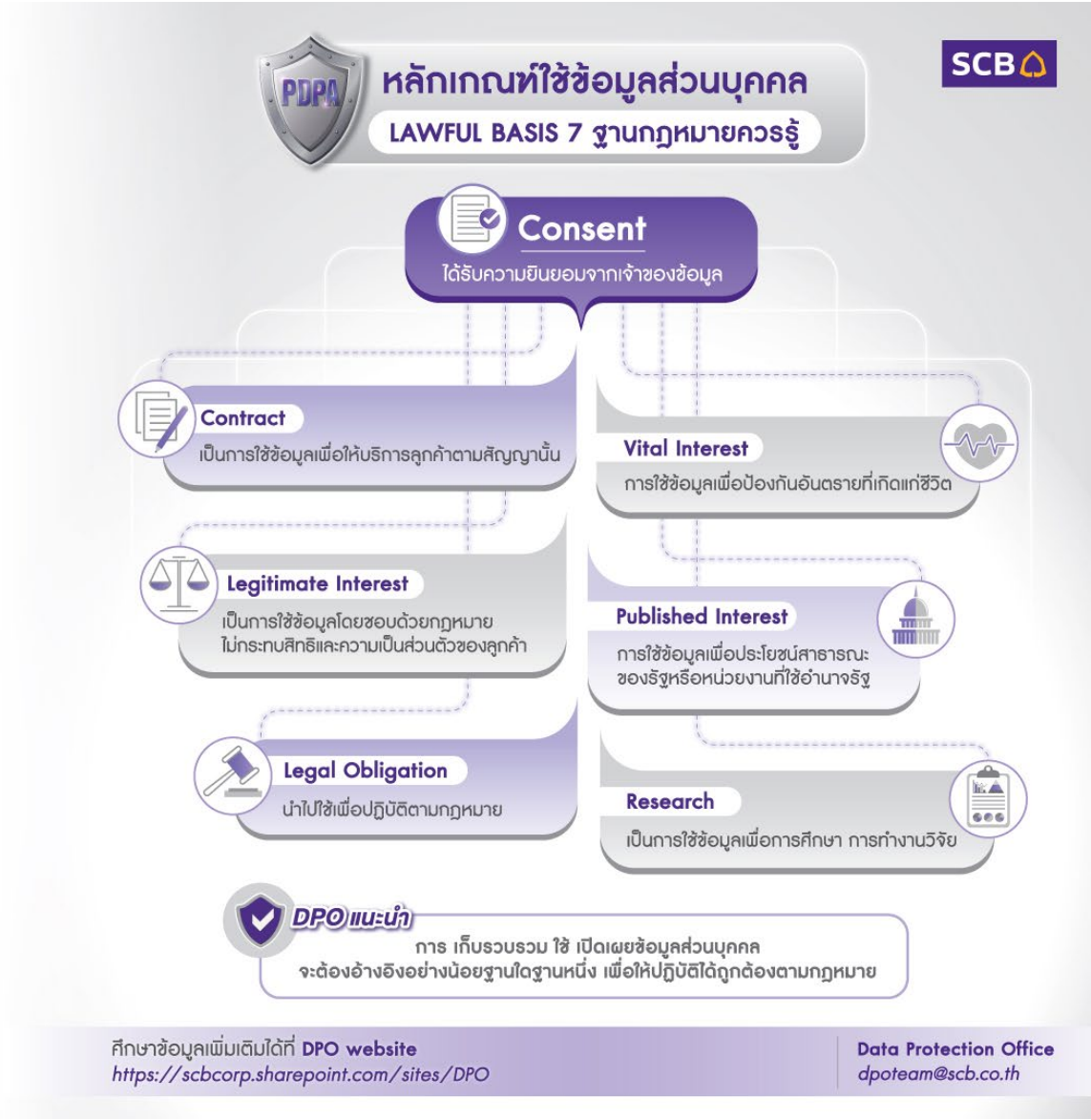
DPO Website


SCB ไทยพาณิชย์
SharePoint
Search
DPO INFORMATION SECURITY, DATA PROTECTION AND OPERATIONAL RISK MANAGEMENT
PDPA
Staff Only
Edit
Share
New
Send to
Page details
Analytics
Published 5/14/2021
Edit
PDPA
การคุ้มครอง
ข้อมูลส่วนบุคคล
PERSONAL DATA PROTECTION
DPO Website
PDPA คืออะไร..?
ทำความรู้จัก และเข้าใจหลักฟันฐานของกฎหมาย พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
(PDPA : Personal Data Protection Act)
LEARNING
เรียนรู้และเข้าใจหลักกฎหมาย และแนวปฏิบัติที่ถูกต้อง
o คลิปวิดีโอ เพื่อการเรียนรู้ สำหรับ ผู้บริหาร พนักงาน และ Privacy Champion
o รายชื่อ Privacy Champion และบทบาทหน้าที่
ข้อมูล
เพื่อการปฏิบัติงาน
o ประกาศ นโยบาย และเอียดคำสั่ง ที่เกี่ยวข้อง
o รวมแบบฟอร์มสำหรับงาน PDPA
o คู่มือและแนวปฏิบัติงานสำหรับสาขา และหน่วยงาน
o Q&A ถาม-ตอบ ข้อสงสัยที่ควรรู้
See all
See all
สาระสำคัญ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
PAIROTH ARDYAMSROUN
Edited 27 เมษายน
Privacy Champion
PAIROTH ARDYAMSROUN
Edited Apr 5, 2021
DIR Processing List
PAIROTH ARDYAMSROUN
Edited 18 กุมภาพันธ์
PDPA สำคัญอย่างไร
PAIROTH ARDYAMSROUN
Edited 27 เมษายน
VDO เพื่อการเรียนรู้สำหรับพนักงาน
PAIROTH ARDYAMSROUN
Edited Feb 18, 2021
แนวปฏิบัติการคุ้มครองข้อม...รกิจธนาคาร สมาคมธนาคารไทย
PAIROTH ARDYAMSROUN
Edited 30 เมษายน
PDPA Overview
PAIROTH ARDYAMSROUN
Edited 19 สิงหาคม, 2563
หลักสูตร PDPA สำหรับผู้บริหาร
PAIROTH ARDYAMSROUN
Edited Dec 14, 2020
รวมแบบฟอร์มและข้อมูลเพื่อการปฏิบัติงาน
PAIROTH ARDYAMSROUN
Edited 6 days ago
หลักพื้นฐาน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPD Principles)
PAIROTH ARDYAMSROUN
Edited 29 เมษายน

Desktop screen



Desktop screen



Desktop screen