การคุ้มครองข้อมูลส่วนบุคคล จากประสบการณ์ SCB

โดย ณัฏฐกานต์ ครรภาฉาย
ผู้ช่วยผู้จัดการใหญ่ งานกฎหมาย
ธนาคารไทยพาณิชย์
25 กันยายน 2561

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับธนาคารพาณิชย์

พระราชบัญญัติการประกอบธุรกิจ
ข้อมูลเครดิต พ.ศ.2545

ประกาศธนาคารแห่งประเทศไทย ที่ สกส. 1/2561
เรื่อง การบริหารจัดการด้านการให้บริการ
แก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

พระราชบัญญัติธุรกิจสถาบันการเงิน
พ.ศ.2551

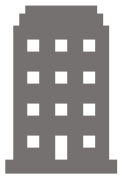
ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2559
เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยี
สารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับธนาคารพาณิชย์

พระราชบัญญัติ
ธุรกิจสถาบันการเงิน
(มาตรา 155)

ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของสถาบันการเงินโดยเหตุที่เป็นผู้มีอำนาจในการจัดการหรือเป็นพนักงาน และเปิดเผยความลับนั้นในประการที่น่าจะก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับธนาคารพาณิชย์



พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต

(มาตรา 20)

ให้บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์สินเชื่อและการออกบัตรเครดิต โดยในการเปิดเผยหรือให้ข้อมูลดังกล่าวจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนทุกครั้ง เว้นแต่เจ้าของข้อมูลได้ให้ความยินยอมไว้เป็นอย่างอื่น ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนด

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับธนาคารพาณิชย์

ประกาศธนาคารแห่งประเทศไทย
ที่ สนส. 19/2559
(เรื่อง การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน)

- ข้อ 5.5.1(3)(3.2) สถาบันการเงินต้องจัดให้มีการทำสัญญาการใช้บริการกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร ซึ่งข้อสัญญาต้องครอบคลุมมาตรฐานของการปฏิบัติงานขั้นต่ำ (เช่น มาตรฐานด้านการรักษาความปลอดภัยและความลับของข้อมูล การห้ามนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้)

- ข้อ 5.5.1(7)(7.1) สถาบันการเงินต้องมั่นใจว่า ผู้ให้บริการภายนอกจะไม่นำข้อมูลของผู้ใช้บริการของสถาบันการเงินหรือข้อมูลของสถาบันการเงินไปเปิดเผยให้กับบุคคลอื่นใด โดยไม่ได้รับความยินยอมจากสถาบันการเงิน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับธนาคารพาณิชย์

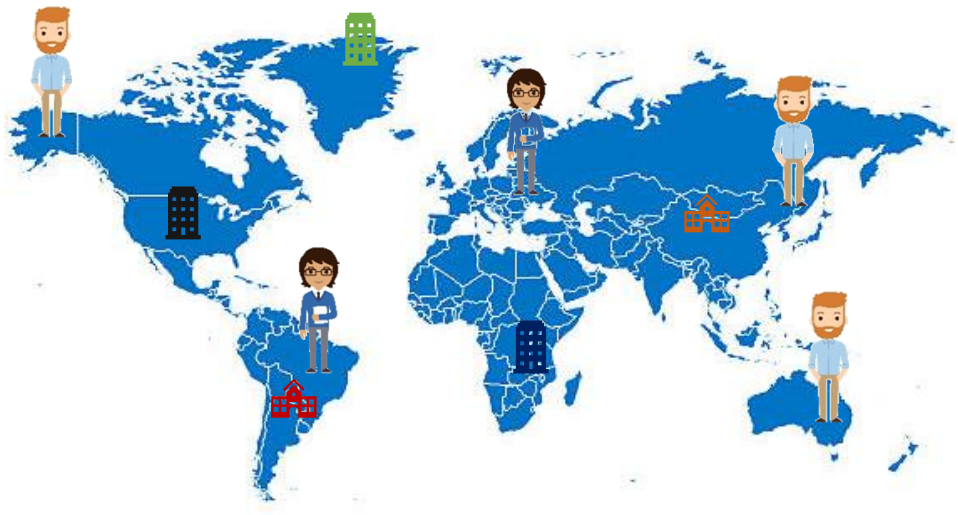
ประกาศธนาคารแห่งประเทศไทย
ที่ สกส. 1/2561
(เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct))

ข้อ 6.2.2(2) ในการเปิดเผยข้อมูลลูกค้าให้บุคคลอื่นเพื่อวัตถุประสงค์ทางการตลาด

(2.1) ให้ขอความยินยอมโดยให้สิทธิลูกค้าเลือกเปิดเผยข้อมูลอย่างชัดเจน ในรูปแบบที่ทำให้มั่นใจได้ว่าลูกค้าเป็นผู้ตัดสินใจให้สิทธิด้วยตนเองและลูกค้าเข้าใจได้ง่ายว่าไม่ใช่เงื่อนไขการใช้ผลิตภัณฑ์ เช่น แยกส่วนที่ขอความยินยอมเพื่อวัตถุประสงค์ทางการตลาดและเพื่อวัตถุประสงค์อื่นที่ไม่ใช่การตลาดออกจากกัน มีถ้อยคำระบุไว้ที่ด้านบนแบบฟอร์มการขอความยินยอมว่าไม่มีผลต่อการพิจารณาการใช้ผลิตภัณฑ์

(2.2) แจ้งวัตถุประสงค์การขอความยินยอมเพื่อการตลาดให้ลูกค้าทราบอย่างชัดเจน

ขอบเขตการบังคับใช้ GENERAL DATA PROTECTION REGULATION (GDPR)



WHO DOES IT APPLY TO?

DATA SUBJECT

DATA CONTROLLER

DATA PROCESSOR

Article 3 – Territorial Scope

1. Controller or Processor in the Union

2. Controller or Processor not established in the Union, but the processing activities related to:
   - offering of goods or services to data subjects in the Union; or
   - monitoring of their behavior as far as their behavior takes place within the Union.

GDPR ใช้บังคับกับธนาคารพาณิชย์ในไทย หากเข้าเกณฑ์ดังต่อไปนี้

เป็น Data Controller หรือ Data Processor

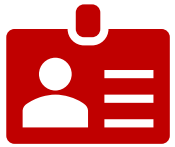
มีสาขาหรือสำนักงานใน EU

เสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลใน EU

ติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลใน EU

มีการทำธุรกรรมกับลูกค้า/คู่ค้าที่ต้องปฏิบัติตาม GDPR เช่น Correspondence Bank ใน EU

ข้อมูลส่วนบุคคล



ข้อมูลส่วนบุคคลของลูกค้า

ได้รับจาก Customer Touch Point เช่น สาขา, Call Center, Mobile Application

ข้อมูลส่วนบุคคลของพนักงาน

ได้รับจากการจ้างงาน

ข้อมูลส่วนบุคคลอื่นๆ

ได้รับจากคู่ค้า

GDPR และ ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

General Data Protection Regulation (GDPR)

Article 3. Territorial Scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (b) the monitoring of their behavior as far as their behavior takes place within the Union.

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....

มาตรา 5

พระราชบัญญัตินี้ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือ การเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม การใช้ หรือการเปิดเผยนั้นได้กระทำในหรือนอกราชอาณาจักร

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมดังต่อไปนี้

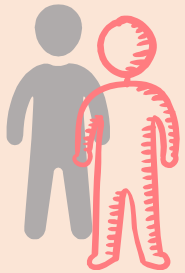
(1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

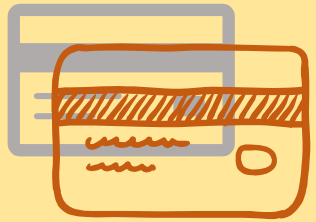
ผลกระทบต่อ Core Banking Area

มาตรการคุ้มครองข้อมูลส่วนบุคคล

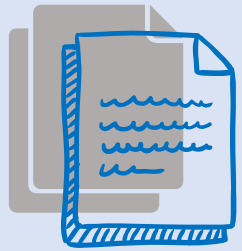
นโยบายการคุ้มครองข้อมูลส่วนบุคคล



สิทธิของเจ้าของ
ข้อมูลส่วนบุคคล



การจัดการข้อมูลส่วนบุคคล
(เก็บรวบรวม ใช้ เปิดเผย)



Data Privacy Notice

สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม GDPR และ ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

RIGHT TO BE INFORMED

RIGHT TO BE FORGOTTEN

RIGHT OF ACCESS

RIGHT TO OBJECT TO PROCESSING

RIGHT TO RECTIFICATION

RIGHT RELATED TO AUTOMATED DECISION MAKING

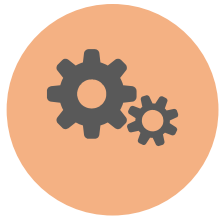
RIGHT TO DATA PORTABILITY

RIGHT TO RESTRICT OF PROCESSING

มาตรการคุ้มครองข้อมูลส่วนบุคคล

TECHNICAL AND ORGANIZATIONAL MEASURES

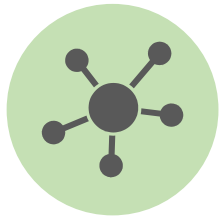
Data Security Measures



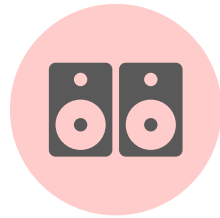
IT Security System

Data Protection Impact Assessment (DPIA)

Data Retention and Back Up



Data Protection by Design and by Default



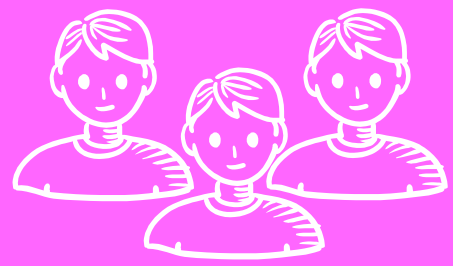
Records of Processing Activities

มาตรการคุ้มครองข้อมูลส่วนบุคคล

การแต่งตั้ง
DATA PROTECTION OFFICER

ความยินยอมของเจ้าของข้อมูล

- แบบความยินยอม
- ช่องทางยกเลิก



การโอนข้อมูล

- การโอนข้อมูลข้ามประเทศ
- สัญญาที่ทำกับ Third Parties

หลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคล

CONSENT

Data subject has given consent to processing of his/her personal data.

VITAL INTERESTS

Processing is necessary to protect someone's life.

CONTRACT

Processing is necessary to fulfil a contractual obligation.

PUBLIC INTEREST

Processing is necessary for public interest.

LEGAL OBLIGATION

Processing is necessary for the controller's compliance with laws or statutory obligation.

LEGITIMATE INTERESTS

Except the interests are overridden by the interests or fundamental rights and freedoms of data subject.

THANK YOU


FULL NAME
AGE
GENDER
TELEPHONE NUMBER
TAX INFO
ADDRESS
CITIZENSHIP
BIRTH DATE
EDUCATION
TRAVEL DOCUMENT
NATIONAL IDENTITY NUMBER
CRIMINAL RECORD
NATIONALITY
MARITAL STATUS
INCOME INFO
IDENTITY DOCUMENT
BANK ACCOUNT NUMBER
VISA INFO