การส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนของประเทศไทย

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 และ 29
และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ ตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ ตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

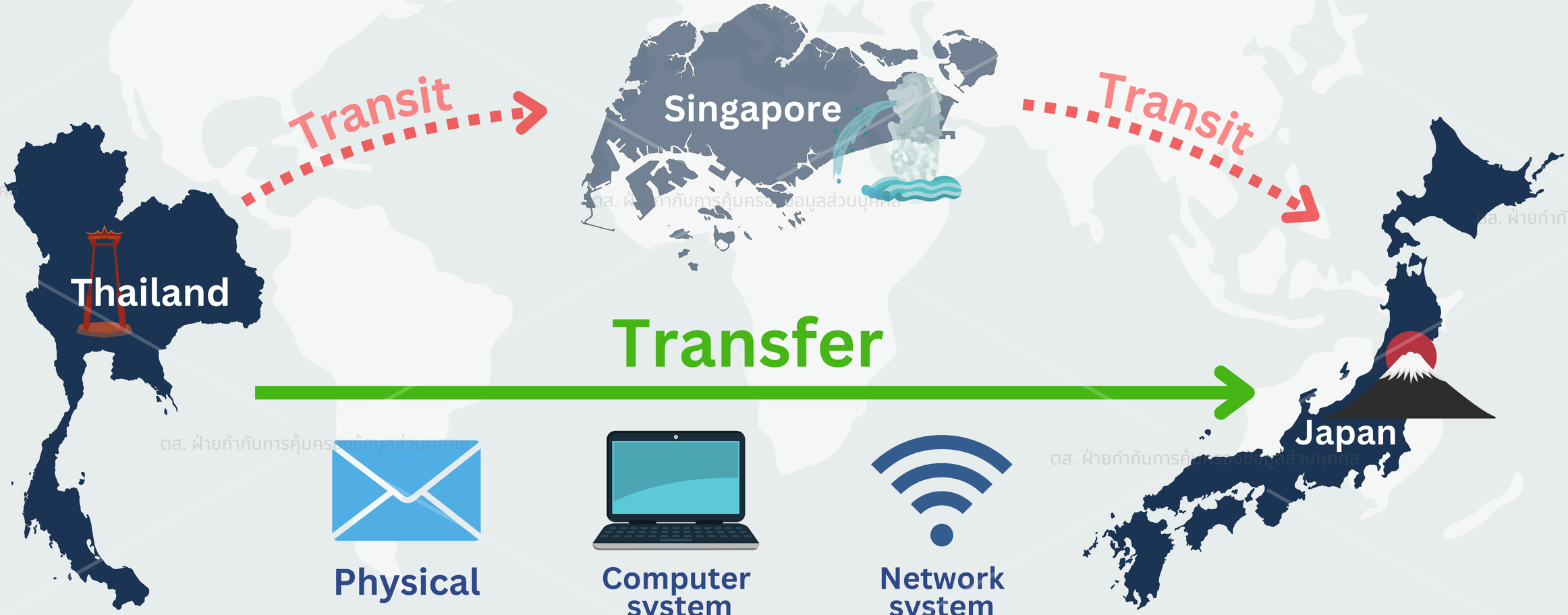
Presented By สำนักตรวจสอบและกำกับดูแล ฝ่ายกำกับการคุ้มครองข้อมูลส่วนบุคคล

การส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนของประเทศไทย

- Intermediary
- Data transit
- Data storage

IaaS PaaS SaaS DSaaS
FaaS Serverless Computing

กรณีไม่มีบุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลได้



เครื่องมือสำหรับการส่งหรือโอนข้อมูลส่วนบุคคล

1 Adequacy
มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ม.28 วรรค 1
+
ประกาศ กคส. เรื่อง หลักเกณฑ์การโอนข้อมูลฯ ตาม ม.28

2 Derogations
ข้อยกเว้น

ม.28 (1) - (6)

DC

3 BCRs
Binding Corporate Rules
นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือธุรกิจเดียวกัน

ม.29 วรรค 1 และ 2

4 Appropriate Safeguards
มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

ม.29 วรรค 3

DP

โทษทางปกครอง

DC

ม.83 โทษปรับ ไม่เกิน 3 ล้านบาท
ม.84 โทษปรับ ไม่เกิน 5 ล้านบาท
(ข้อมูลอ่อนไหว)

DP

ม.86 โทษปรับ ไม่เกิน 3 ล้านบาท
ม.87 โทษปรับ ไม่เกิน 5 ล้านบาท
(ข้อมูลอ่อนไหว)

สำนักตรวจสอบและกำกับดูแล ฝ่ายกำกับการคุ้มครองข้อมูลส่วนบุคคล Up Date ณ 12 ตุลาคม 2567

1 A Adequacy

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

พิจารณาจากข้อเท็จจริงเกี่ยวกับความพอเพียงของปัจจัย

มาตรการหรือกลไก ทางกฎหมาย ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องกับ PDPA ของประเทศไทย โดยเฉพาะ

- หน้าที่ของ DC ที่ต้องจัดให้มี Security
- มาตรการคุ้มครองข้อมูลที่เหมาะสม และสามารถบังคับตามสิทธิของ DS ได้
- มาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

มีหน่วยงานหรือองค์กรบังคับใช้กฎหมายในประเทศปลายทาง หรือองค์การระหว่างประเทศ (Regulator)

2D Derogations
ข้อยกเว้น

1. เป็นการปฏิบัติตามกฎหมาย
2. ได้รับความยินยอม โดยได้แจ้งให้ทราบถึงมาตรฐานที่ไม่เพียงพอ
3. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญา
4. เป็นการกระทำตามสัญญาระหว่าง DC กับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของ DS
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของ DS ในขณะที่ไม่สามารถให้ความยินยอมได้
6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

3 BCRs

Binding Corporate Rules
นโยบายในการคุ้มครองข้อมูลส่วนบุคคล ในเครือกิจการหรือธุรกิจเดียวกัน

นโยบายการคุ้มครองข้อมูลส่วนบุคคล
ได้รับการตรวจสอบ และรับรองจาก สคส. แล้ว

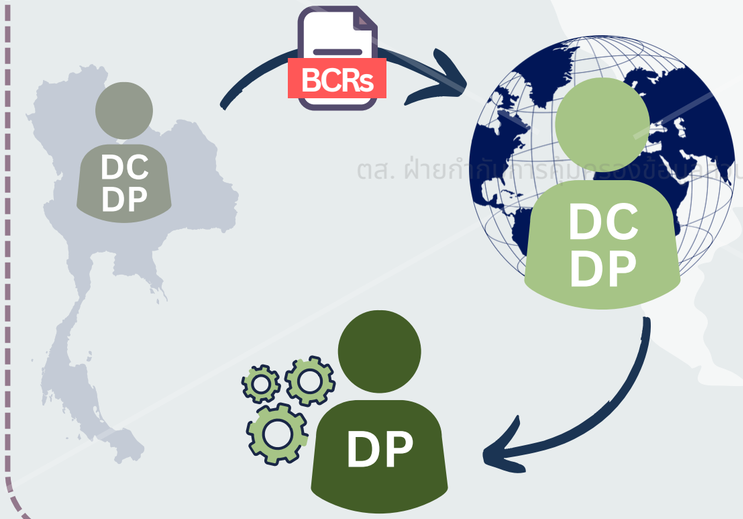
สำนักตรวจสอบและกำกับดูแล ฝ่ายกำกับการคุ้มครองข้อมูลส่วนบุคคล Up Date ณ 12 ตุลาคม 2567

ข้อ 7

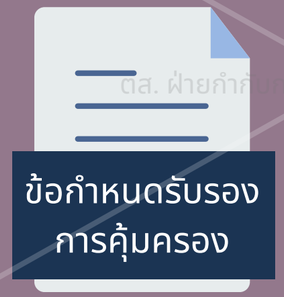
หลักเกณฑ์และวิธีการตรวจสอบและรับรอง นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน โดยมีเนื้อหาสาระของ BCRs ว่าต้องเป็นไปตามหลักเกณฑ์

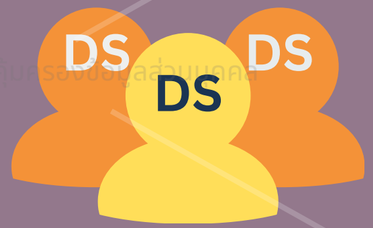
1

การมีผลและสภาพบังคับในทางกฎหมาย ของ BCRs กับนิติบุคคลหรือบุคคล ธรรมดาในเครือกิจการหรือบุคคลเครือ ธุรกิจเดียวกัน ตลอดจน DP ที่เกี่ยวข้อง



2





สิทธิและการร้องเรียน

สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน ไปยังต่างประเทศ

3

- มีมาตรการในการคุ้มครองข้อมูล ส่วนบุคคล และมาตรการ Security ที่สอดคล้องกับ PDPA

โดยมาตรการ Security จะต้องเป็นไป ตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด

[ม.37(1) + ประกาศ กคส. เรื่อง Security]

4 AS

Appropriate Safeguards

มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

อาจอยู่ในรูปแบบ ดังนี้

ข้อสัญญา

การรับรอง (Certification)

ข้อกำหนดการคุ้มครองฯในตราสารหรือข้อตกลงทางกฎหมาย

ข้อ 9

(1) การมีผลและสภาพบังคับในทางกฎหมาย

(2) ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล

(3) มีมาตรการที่สอดคล้องกับ PDPA โดยมาตรการ Security ต้องเป็นไปตาม PDPA ด้วย (ม.37(1)) + ประกาศ กคส. เรื่อง Security

ข้อสัญญา

มีเนื้อหาตาม ข้อ 10 (1)
ตามประกาศ กคส.
เรื่อง หลักเกณฑ์การส่งหรือโอน
ข้อมูลไปต่างประเทศ ตาม ม.29

ข้อสัญญาที่จัดทำขึ้น
ตามกฎหมายของต่างประเทศ
โดยใช้ข้อสัญญาต้นแบบ
อย่างใดอย่างหนึ่ง

ข้อสัญญาอื่นๆ
ตามที่ กคส.
ประกาศกำหนด

มีเนื้อหาตาม
ข้อ 11 (1)
ตามประกาศ กคส.
เรื่อง หลักเกณฑ์
การส่งหรือ
โอนข้อมูล
ไปต่างประเทศ
ตาม ม.29

ข้อ 10

ข้อสัญญาต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(ก) การเก็บรวบรวม ใช้ และเปิดเผย รวมถึงการโอน ต้องเป็นไปตาม PDPA

(ข) ผู้ส่งหรือผู้โอน และผู้รับข้อมูลฯ ต้องจัดให้มีมาตรการ Security ที่เป็นไปตามมาตรฐานขั้นต่ำตาม PDPA

(ค) กรณีผู้รับข้อมูลฯ เป็น DP

(1)

- ดำเนินการตามคำสั่งหรือในนามของผู้ส่งหรือผู้โอน และตามวัตถุประสงค์ที่ผู้ส่งหรือผู้โอนกำหนดไว้เท่านั้น
- ผู้รับต้องแจ้งผู้ส่งหรือผู้โอน หากมีการขอใช้สิทธิของ DS ตามกฎหมาย เว้นแต่ ผู้ส่งหรือผู้โอนได้มอบหมายให้ผู้รับสามารถดำเนินการตามคำขอแทน
- ต้องส่งคืนข้อมูลฯ ตามสัญญาแก่ผู้ส่งหรือผู้โอน หรือลบหรือทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ โดยวิธีการที่เหมาะสม และต้องยืนยันเป็นลายลักษณ์อักษรต่อผู้ส่งหรือผู้โอน
- ต้องแจ้งเหตุละเมิดฯ แก่ผู้ส่งหรือผู้โอนโดยไม่ชักช้า ภายใน 72 ชม. นับแต่ทราบเหตุ

ข้อ 10

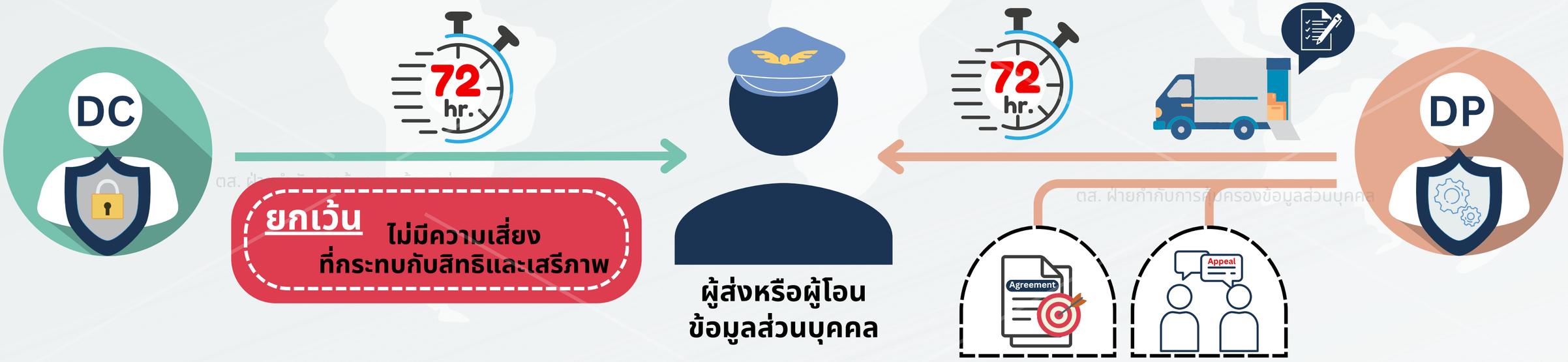
ข้อสัญญาต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้ (ต่อ)

(1)

(ง) กรณีผู้รับข้อมูลฯ เป็น DC

ต้องแจ้งเหตุละเมิดฯ แก่ผู้ส่งหรือผู้โอนโดยไม่ชักช้า <u>ภายใน 72 ชม.</u> นับแต่ทราบเหตุ
เว้นแต่ การละเมิดดังกล่าวไม่มีความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพ

(จ) ต้องมีมาตรการเยียวยาทางกฎหมายแก่ DS ที่มีประสิทธิภาพ (Effective legal remedies)



ข้อ 10

ข้อสัญญาต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้ (ต่อ)

(2)

ข้อสัญญาที่จัดทำขึ้นตามกฎหมายของต่างประเทศ โดยใช้ข้อสัญญาต้นแบบอย่างใดอย่างหนึ่ง ดังนี้

ASEAN Model Contractual Clauses for Cross Border Data Flows

Standard Contractual Clauses for the Transfer of Personal Data to third Countries

ข้อสัญญาอื่นๆ ตามที่ กคส. ประกาศกำหนด

ข้อ 11

1. มาตรการแจ้งการส่งหรือโอนข้อมูลให้ DS ทราบ
2. มาตรการการจำกัดการส่งหรือโอนเท่าที่จำเป็น
3. มาตรการทางเลือกแก่ DS ในการใช้สิทธิ
   - ยกเลิกการส่งหรือโอนข้อมูลฯ ไปยังบุคคลภายนอก
   - ยกเลิกการใช้นอกขอบเขตวัตถุประสงค์
4. มาตรการกำหนดความรับผิดชอบในสัญญา รวมถึงการคุ้มครองการส่งหรือโอนข้อมูลไปยังบุคคลภายนอก
5. มาตรการ Security
6. มาตรการการกำหนดสิทธิการเข้าถึงข้อมูล การดำเนินการให้ข้อมูลนั้นถูกต้อง สมบูรณ์ และเป็นปัจจุบัน และการลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้
7. มาตรการเยียวยาความเสียหายที่มีประสิทธิภาพ

สรุปเครื่องมือในการส่งหรือโอนข้อมูลส่วนบุคคล

A
Adequacy

มีกลไกทางกฎหมาย
ที่สอดคล้องกับ PDPA

REGULATOR

DS Right
Entreatment

SECURITY
มาตรการหรือกลไก ทางกฎหมาย
ที่เกี่ยวกับการคุ้มครองข้อมูลส่วน
บุคคลสอดคล้องกับ PDPA
ของประเทศไทย โดยเฉพาะ

D
Derogations

ตามกฎหมาย

Consent

Contract

Contract ระหว่าง DC
กับบุคคลหรือนิติบุคคลอื่น
เพื่อประโยชน์ของ DS

ระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
ในกรณี DS ให้ความยินยอมไม่ได้

เพื่อประโยชน์สาธารณะที่สำคัญ

BCRs
Binding Corporate Rules

มีผลและ
สภาพบังคับ
ในทางกฎหมาย

มีมาตรการในการคุ้มครองข้อมูล
ส่วนบุคคล และมาตรการ Security
ที่สอดคล้องกับ PDPA
ตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด
(ม.37(1))

ข้อกำหนดรับรอง
การคุ้มครอง

DS DS DS
สิทธิและการร้องเรียน

สำหรับข้อมูลส่วนบุคคล
ที่ถูกส่งหรือโอนไปต่างประเทศ

AS
Appropriate Safeguards

มีลักษณะ
อย่างใดอย่างหนึ่ง

มีเนื้อหาตาม ข้อ 10 (1)
ตามประกาศ กคส.
เรื่อง หลักเกณฑ์การส่งหรือโอน
ข้อมูลไปต่างประเทศ ตาม ม.29

ข้อสัญญาที่จัดทำขึ้นตามกฎหมายของต่างประเทศ
โดยใช้ข้อสัญญาต้นแบบอย่างใดอย่างหนึ่ง

MCCs
SCCs
CERTIFIED
ข้อสัญญาอื่นๆ
ตามที่ กคส.
ประกาศกำหนด

มีเนื้อหาตาม ข้อ 11 (1) ตามประกาศ กคส.
เรื่อง หลักเกณฑ์การส่งหรือโอนข้อมูลไปต่างประเทศ ตาม ม.29

CONTRACT
ข้อสัญญา

Certification
การรับรอง
(Certification)

Requirements
ข้อกำหนด
การคุ้มครองฯในตราสาร
หรือข้อตกลงทางกฎหมาย

(1) การมีผลและสภาพบังคับ
ในทางกฎหมาย

(2) ข้อกำหนดที่รับรองการคุ้มครอง
ข้อมูลส่วนบุคคล

(3) มีมาตรการที่สอดคล้องกับ PDPA
โดยมาตรการ Securityต้องเป็นไปตาม PDPA ด้วย
(ม.37(1)) + ประกาศ กคส. เรื่อง Security

DC สามารถใช้เครื่องมือได้ทั้ง 4 เครื่องมือ
แต่ DP สามารถใช้เครื่องมือได้เฉพาะ BCRs และ AS

สำนักตรวจสอบและกำกับดูแล ฝ่ายกำกับการคุ้มครองข้อมูลส่วนบุคคล Up Date ณ 12 ตุลาคม 2567

สคส.

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล