ความรู้เบื้องต้นเกี่ยวกับ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

อ. ดร. พีรพัฒ โชคสุวัฒนสกุล

คณะนิติศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

PEERAPAT CHOKESUWATTANASKUL

DBA., PHD. (CAMBRIDGE)

- Lecturer in Law and Economics, Faculty of Law, Chulalongkorn University
- Co-author of Thailand Data Protection Guidelines 2.0 and the series of training with over 500 professional attendees
- Ex-data scientist, Agoda.com
- Ex-supervisor in Statistics and Econometrics, Trinity Hall College, University of Cambridge
- PDPA consultant for companies and organisations including Builk, TDPK, Villa market, etc.

Faculty of Law, Chulalongkorn University

THAILAND DATA PROTECTION

GUIDELINES 2.0

แนวปฏิบัติเกี่ยวกับการคุ้มครอง
ข้อมูลส่วนบุคคล

Thailand Data Protection Guidelines 2.0

LAW CHULA

LAWYERS WHO KNOW ASIA

Linklaters

CHANDLER MHM

Dherakupt INTERNATIONAL LAW OFFICE LTD.

เค้าโครงการบรรยาย

หลักการพื้นฐานและคำนิยาม

๑๐ อย่างที่คุณต้องรู้เกี่ยวกับข้อมูลส่วนบุคคล

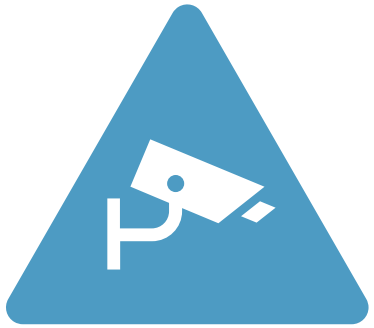
หลักการพื้นฐาน
และ
คำนิยาม

UNIT OF ANALYSIS IS NEVER DATA ALONE.

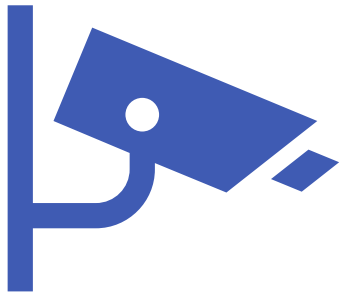
ข้อมูล

วัตถุประสงค์

หลักการสำคัญสองประการ



Privacy



Security

คำนิยาม

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูล เว้นแต่...”

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูล เว้นแต่...”

คำนิยามของข้อมูลส่วนบุคคล

“ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

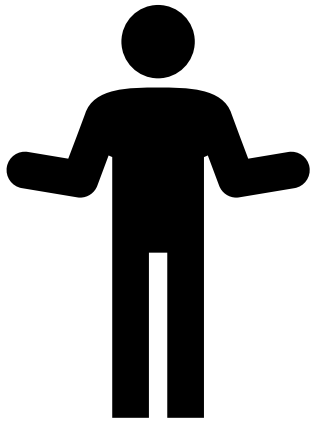
คำนิยามของข้อมูลส่วนบุคคล

“ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

คำนิยามของข้อมูลส่วนบุคคล

“ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

ข้อมูล



บุคคลธรรมดา
ที่ยังมีชีวิต

ชื่อ นามสกุล

รหัสประจำตัว

ที่อยู่ติดต่อ

รหัสประจำเครื่อง

ข้อมูลชีวภาพ

เอกสารแสดงทรัพยสิทธิ

ข้อมูลที่เชื่อมโยงกับข้อมูลอื่นได้

- ข้อมูลประชากร
- ข้อมูลทางการแพทย์

log file

ข้อมูลที่สามารถค้นหาได้

รหัสบริษัท

ข้อมูลนิรนาม*

ข้อมูลผู้เสียชีวิต

ผู้ควมคุมข้อมูล และ ผู้ประมวลผลข้อมูล

CONTROLLER

ตัดสินใจ

เก็บหรือประมวลผลอื่น

วัตถุประสงค์ในการเก็บ

ข้อมูลใดบ้าง

ข้อมูลของเจ้าของข้อมูลใด

ประมวลผลอย่างไร

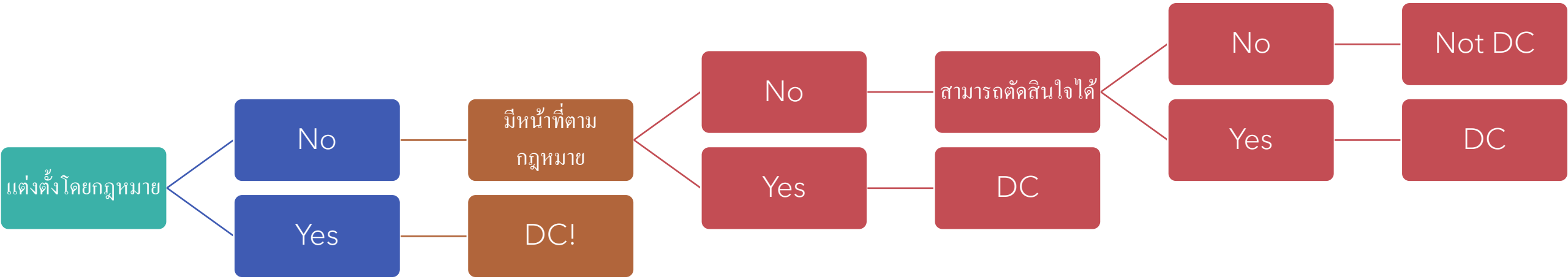
ได้รับประโยชน์ทางการค้า หรือประโยชน์อื่นใดจากการประมวลผลข้อมูลนั้น

ประมวลผลข้อมูลส่วนบุคคลได้ตามสัญญาที่ทำไว้กับเจ้าของข้อมูลส่วนบุคคล

เป็นนายจ้างของเจ้าของข้อมูล

มีความสัมพันธ์โดยตรงกับเจ้าของข้อมูล

มีการแต่งตั้งให้ผู้ประมวลข้อมูลดำเนินการประมวลผลข้อมูลส่วนบุคคล

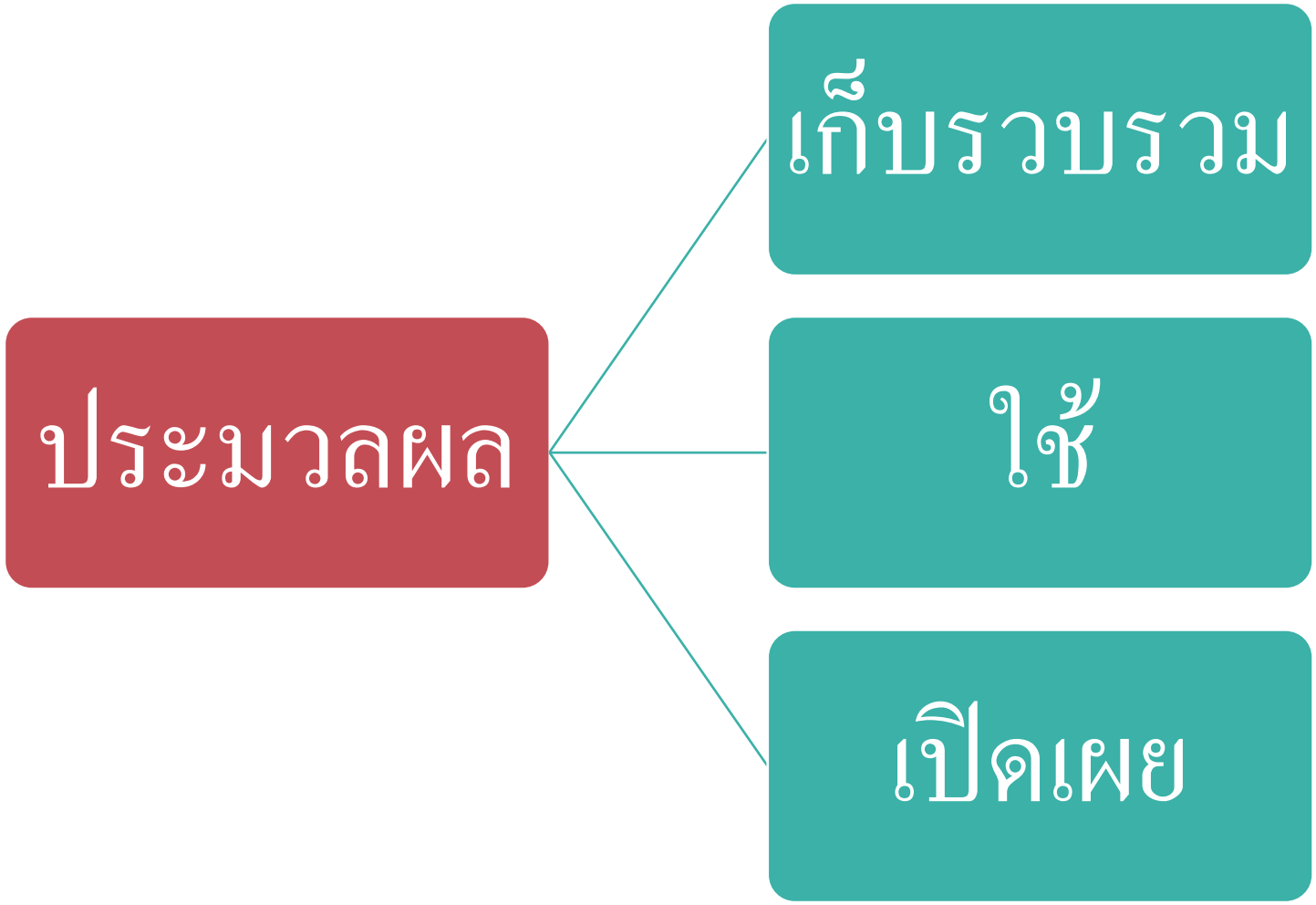

แต่งตั้งโดยกฎหมาย
No
Yes
มีหน้าที่ตามกฎหมาย
DC!
No
Yes
สามารถตัดสินใจได้
DC
No
Yes
Not DC
DC

ผู้ประมวลผลข้อมูล

- เป็นบุคคลต่างหาก
- ไม่ได้มีการตัดสินใจ
- ไม่มีผลประโยชน์โดยตรงจากการประมวลผล (นอกจากค่าตอบแทนจากผู้ควบคุมข้อมูล)

เป็นทั้งคู่ได้หรือไม่?

การประมวลผล?

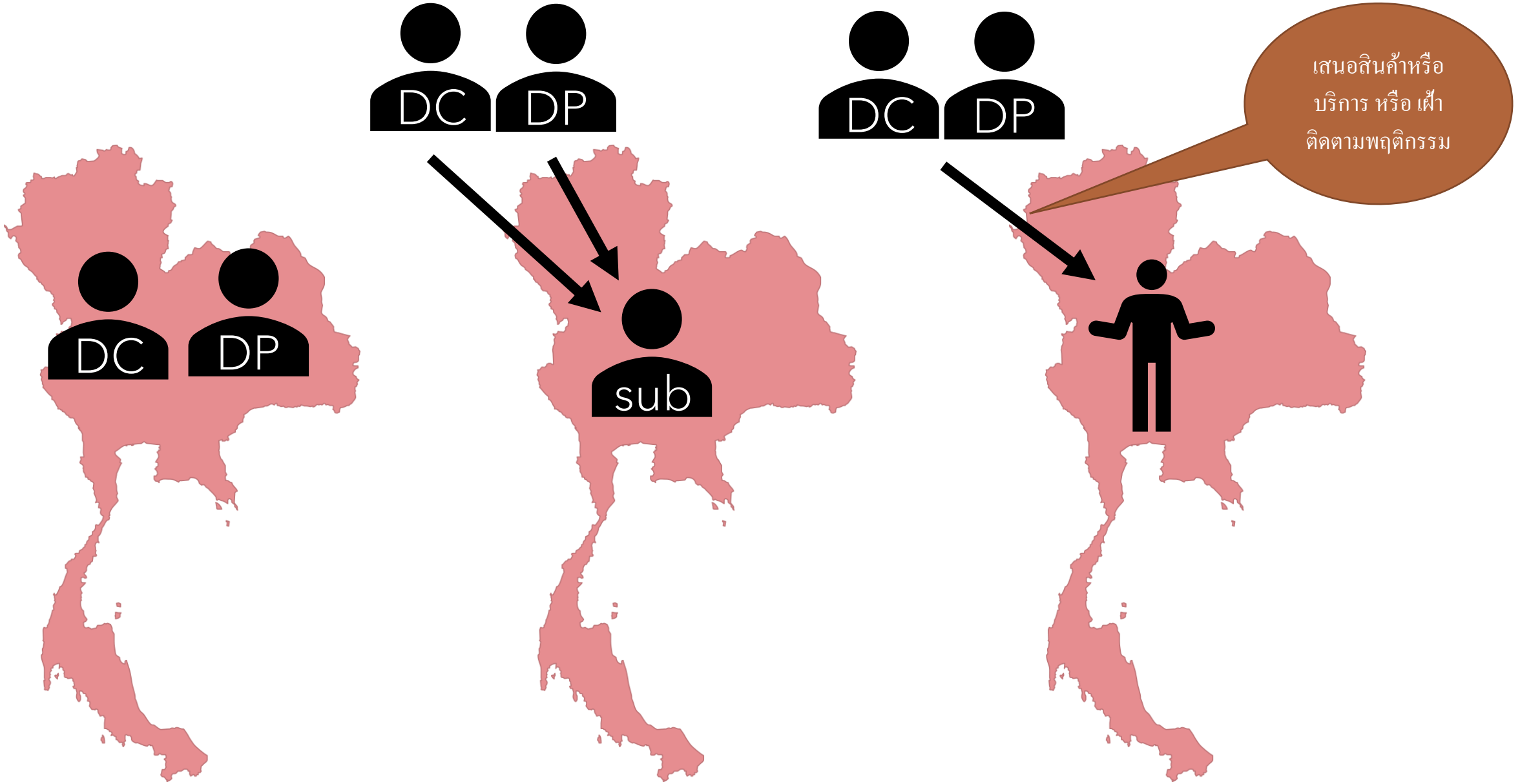

ประมวลผล
เก็บรวบรวม
ใช้
เปิดเผย

เพราะฉะนั้น...

ทำเอง หรือใช้ระบบอัตโนมัติ

“ยุ่ง” กับข้อมูล

รวมถึงการลบและทำลายข้อมูลด้วย


DC
DP
DC
DP
sub
DC
DP
เสนอสินค้าหรือ
บริการ หรือ เฝ้า
ติดตามพฤติกรรม

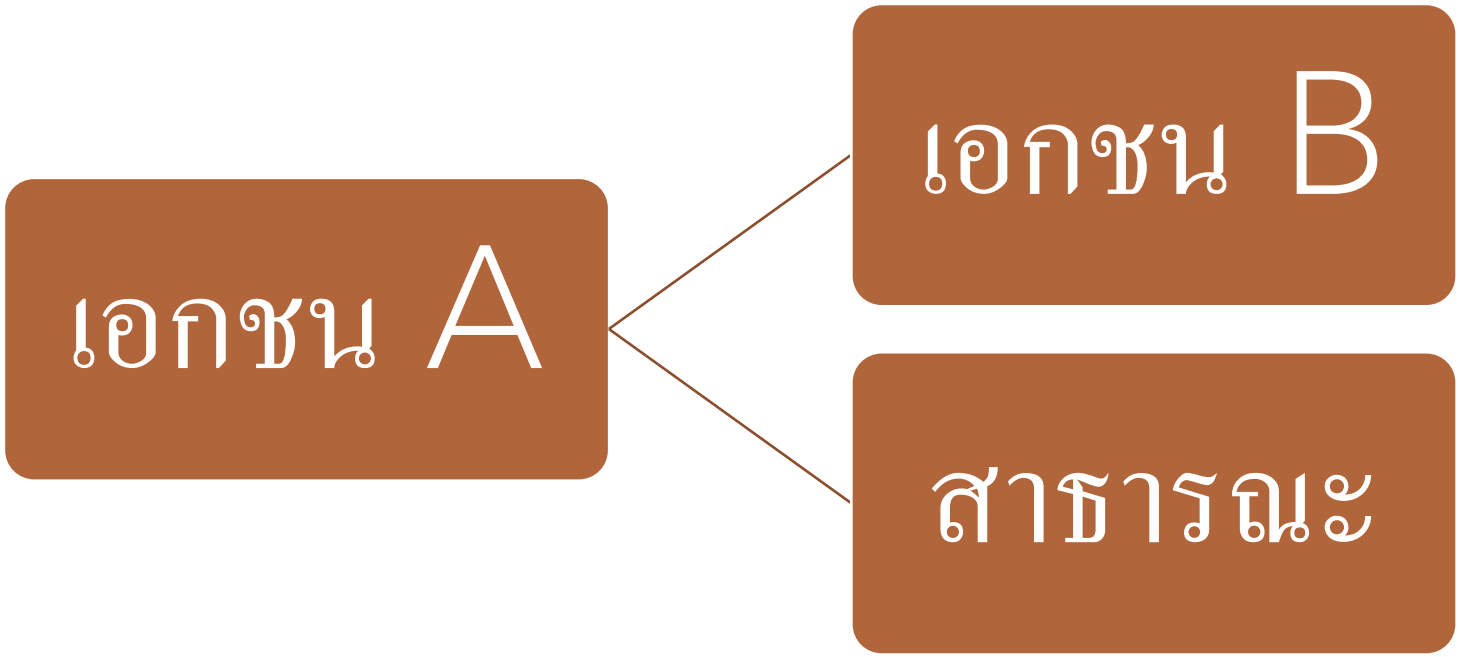
ดังนั้น ...

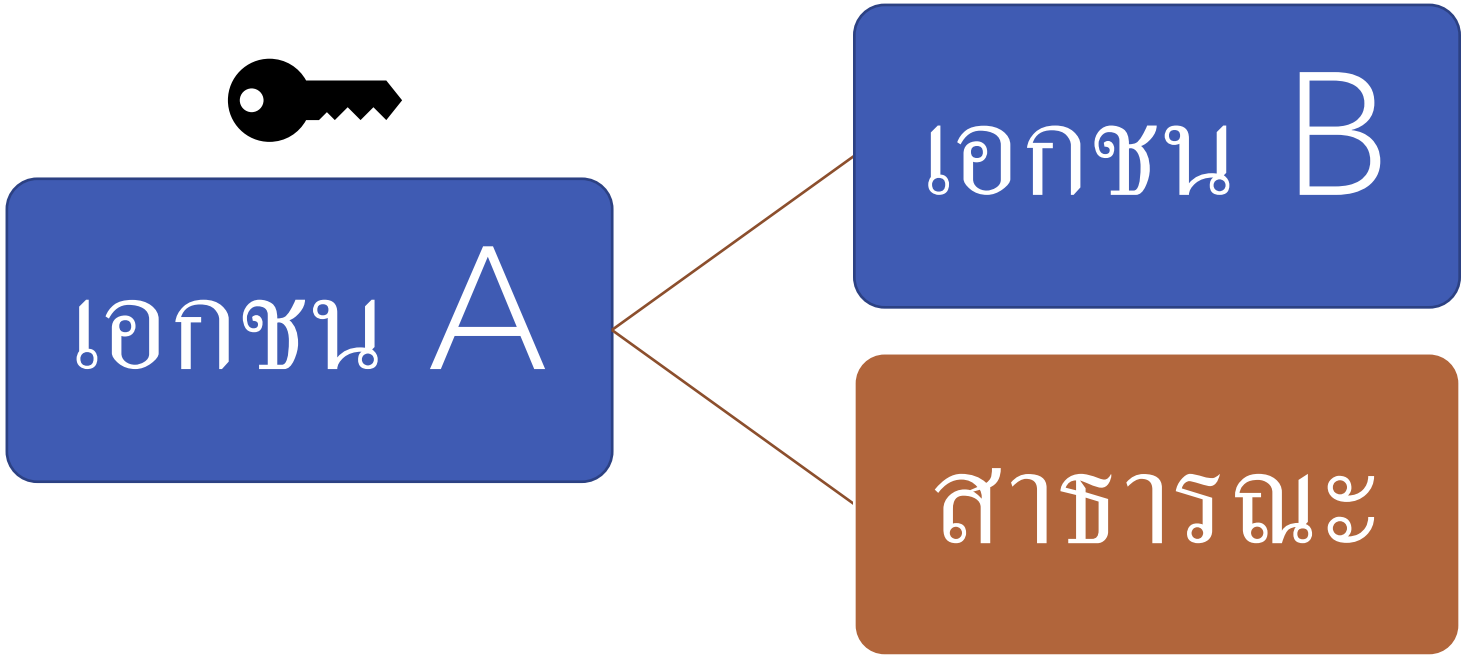
ไม่ได้มีแบบของการประมวลผลกำหนดไว้ตายตัว

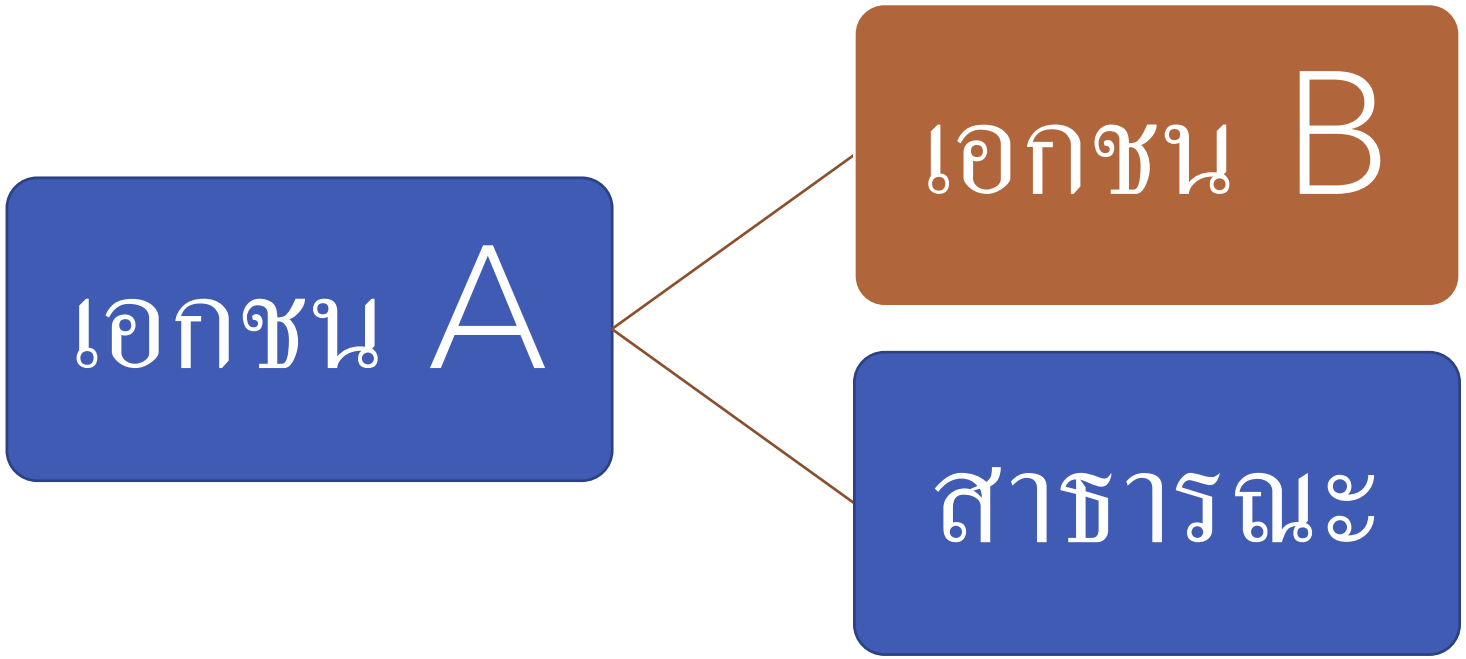
ระบุตัวตนได้ไม่ว่าทางตรงหรือทางอ้อม

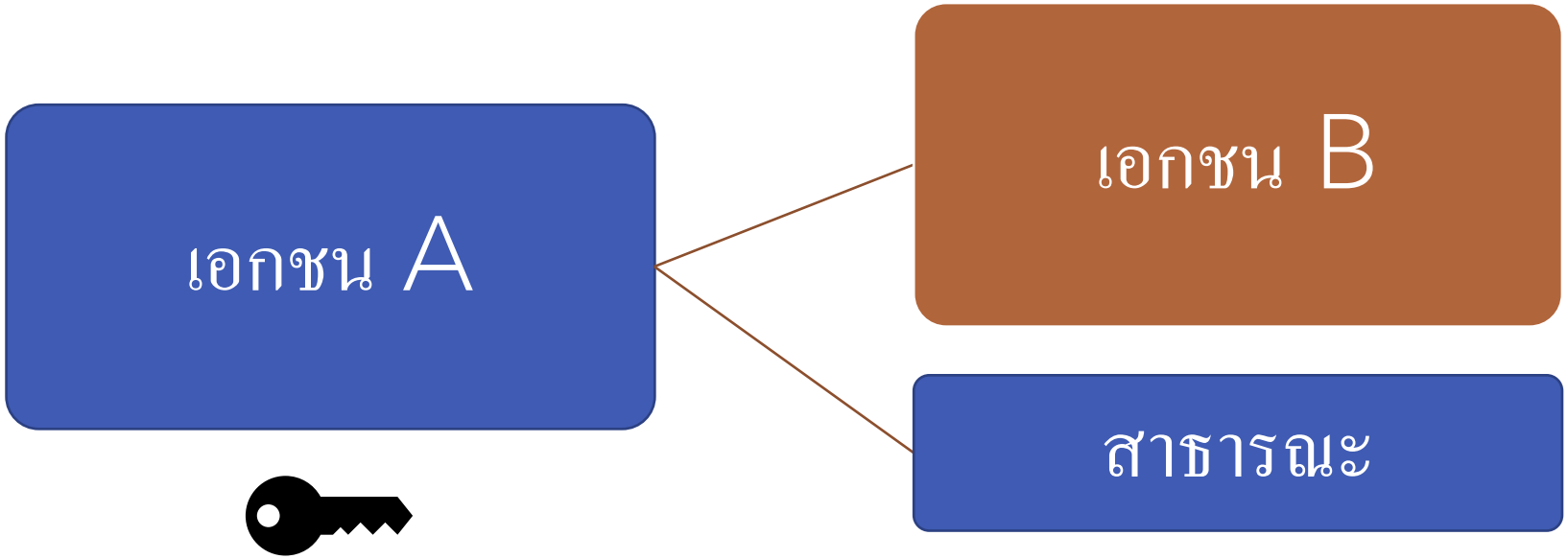
ข้อมูล ไม่จำเป็นต้องเป็นข้อเท็จจริง

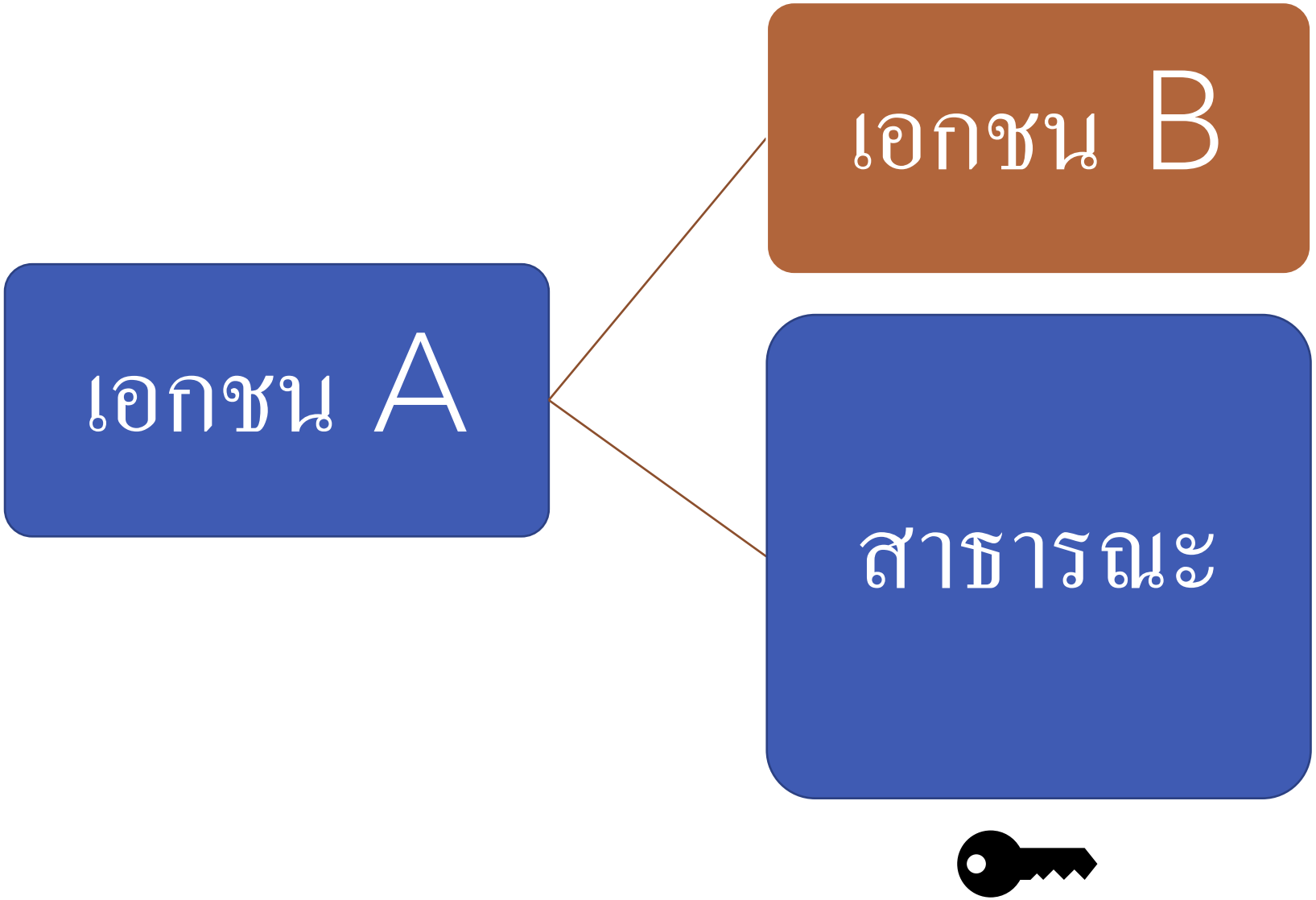
ประโยชน์ส่วนบุคคล VS ประโยชน์สาธารณะ


เอกชน A
เอกชน B
สาธารณะ


เอกชน A
เอกชน B
สาธารณะ


เอกชน A
เอกชน B
สาธารณะ
?


เอกชน A
เอกชน B
สาธารณะ


เอกชน A
เอกชน B
สาธารณะ

ข้อยกเว้น

เพื่อประโยชน์ส่วนตน หรือกิจกรรมในครอบครัวของบุคคลนั้น

หน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ

กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม

สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา คณะกรรมาธิการ

EXEMPTIONS IN ART. 4

- (๑) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล **เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้น**เท่านั้น
- (๒) การดำเนินการของ**หน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ** ซึ่งรวมถึง ความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
- (๓) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะ เพื่อ**กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม**อันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

EXEMPTIONS IN ART. 4

- (๔) **สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการ**ที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
- (๕) **การพิจารณาพิพากษาคดีของศาล**และการดำเนินงานของเจ้าหน้าที่ใน**กระบวนการพิจารณาคดี** การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
- (๖) การดำเนินการกับข้อมูลของ**บริษัทข้อมูลเครดิต**และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

EXEMPTIONS IN ART. 4

- ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (๒) (๓) (๔) (๕) และ (๖) และผู้ควบคุมข้อมูล ส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง **ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย**

SO, AS A GOVERNMENT UNIT, DO I NEED TO CARE? YES

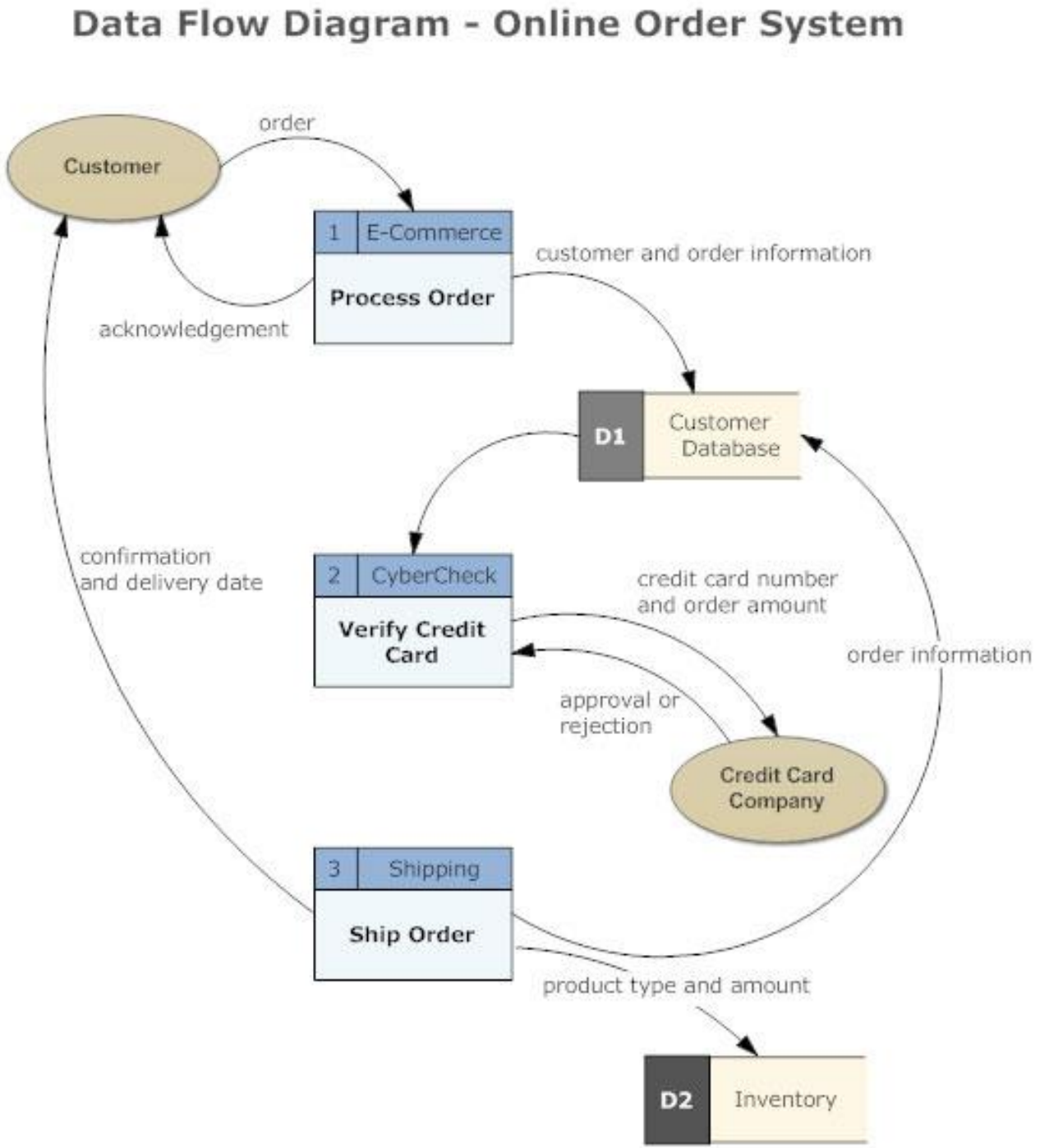
หลักการพื้นฐาน

๑. เข้าใจการไหลของข้อมูลส่วนบุคคล

การค้นหาข้อมูล

การระบุอัตลักษณ์ของข้อมูล

ภายใน



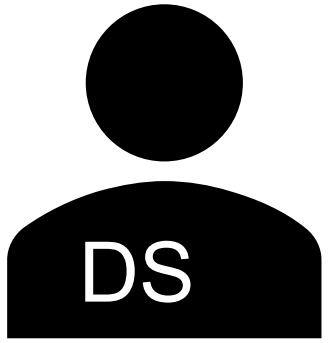
https://www.smartdraw.com/data-flow-diagram/

การค้นหาข้อมูล

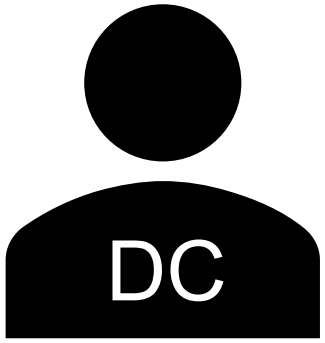
การระบุอัตลักษณ์ของข้อมูล

ภายนอก

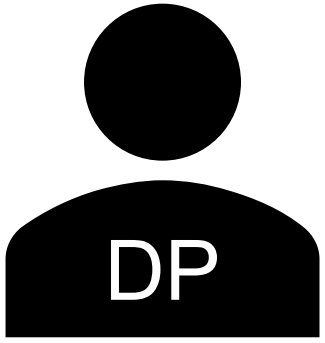
๒. คุณเป็นใครในสายตาของกฎหมาย?



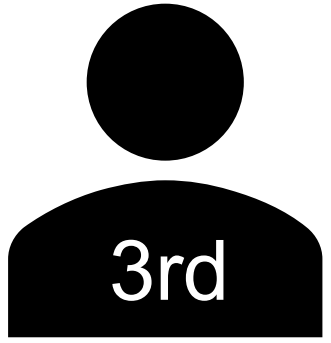
เจ้าของข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูล



ผู้ประมวลผลข้อมูล



บุคคลภายนอก

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

วิธีการในเชิงบริหาร หรือเทคนิค

- กระบวนการ
- ความปลอดภัย
  - การสุญหาย
  - การประมวลผลข้อมูล
  - การเจาะเข้าถึงข้อมูล

ระบบ

- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- DPO
- DPIA

ต่อผู้ประมวลผลข้อมูล

- เลือกคนที่ปลอดภัย
- ทำสัญญาประมวลผลข้อมูลไว้ให้ชัดเจน

การส่งข้อมูล

- ไปต่างประเทศ

ต่อสาธารณะ

- ข้อมูลรั่วไหล
- มีตัวแทนในราชอาณาจักร
- Log process

หน้าที่ของผู้ประมวลผลข้อมูลฯ

วิธีการในเชิงบริหาร หรือเทคนิค

- กระบวนการ
- ความปลอดภัย
  - การสูญหาย
  - การประมวลผลข้อมูล
  - การเจาะเข้าถึงข้อมูล
- DPO

บุคคลภายนอก

- ทำตามผู้ควบคุมข้อมูล
- ไม่มีหน้าที่โดยตรงต่อเจ้าของข้อมูลส่วนบุคคล

ต่อผู้ควบคุมข้อมูล

- แจ้งผู้ควบคุมข้อมูลหากมีวิธีที่ดีกว่าในการรักษาความปลอดภัยของข้อมูล
- จัดทำสัญญาการประมวลผลข้อมูล

ต่อสาธารณะ

- ข้อมูลรั่วไหล
- มีตัวแทนในราชอาณาจักร
- Log process

๓. ฐานทางกฎหมายที่ให้สิทธิ

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูล เว้นแต่...”

ฐานการประมวลผลข้อมูล

ความยินยอม

สัญญา

ผลประโยชน์โดยชอบธรรม

หน้าที่ตามกฎหมาย

ภารกิจของรัฐ

ประโยชน์ต่อชีวิต

วิจัยและสถิติ

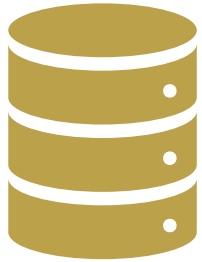
๔. ประเมินความเสี่ยงและหาทางป้องกัน

นอกจากเข้าใจการเคลื่อนที่ของข้อมูลแล้วก็ต้องเข้าใจความเป็นไปได้ในการโจมตี

ระดับของความเสี่ยง

สิ่งแวดล้อม

การเข้าถึงข้อมูล และ กิจกรรม



ข้อมูล

ความยากง่ายในการระบุตัวตน

ปริมาณข้อมูล

ลักษณะของข้อมูล

๕. เก็บทุกอย่างไว้เป็นลายลักษณ์อักษร

ผู้ควบคุม และผู้ประมวลผล จำเป็นต้อง...

ทำตามกฎหมาย

แสดงให้เห็นว่าทำ

นโยบายข้อมูลส่วนบุคคล

อะไรคือข้อมูลส่วนบุคคล

เราเก็บข้อมูลอะไรบ้าง

เราเก็บไว้นานเท่าใด

เราได้ข้อมูลของคุณมาอย่างไร

เรามีวัตถุประสงค์ในการประมวลผลข้อมูลอย่างไรบ้าง

เราประมวลผลข้อมูลอย่างไรบ้าง

เรารักษาความปลอดภัยอย่างไร

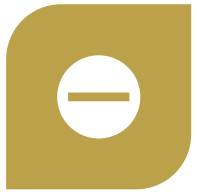
คุณมีสิทธิประการใดบ้าง

ติดต่อใครได้บ้าง

๖. มีกระบวนการให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิ

สิทธิของเจ้าของข้อมูล

ถอนความยินยอม



เข้าถึงข้อมูล

แก้ไขข้อมูลให้ถูกต้อง

ลบข้อมูล

จำกัดการประมวลผล

เคลื่อนย้ายข้อมูล

คัดค้านการประมวลผล

BUT YOU MAY REJECT…

สิทธิ	ฐานในการปฏิเสธ										
	Unfounded	Excessive	Already had	Freedom of opinion expression	Contract	Legal Obligation	Adverse impact on others	Necessary for processing	Public interest, Public task, Law	Legal claim	Legitimate interest
ถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
เข้าถึงข้อมูล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
แก้ไขข้อมูลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
ลบข้อมูล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
จำกัดการประมวลผล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
โอนย้ายข้อมูล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
คัดค้านการประมวลผล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
ไม่ให้ใช้กระบวนการอัตโนมัติในการตัดสินใจ	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

Source: Thailand Data Protection Guideline

๗. ทำสัญญาไว้ให้ชัดเจนถึงขอบเขตการประมวลผล

สัญญาการประมวลผลข้อมูล

- ผู้ประมวลผลข้อมูลพึง
  - ทำตามที่ได้รับคำสั่งเท่านั้น
  - มีมาตรการรักษาความปลอดภัย
  - เก็บรายละเอียดกิจกรรมต่างๆ
  - ทำข้อตกลงการประมวลผลข้อมูล

๘. อำนาจนำมาซึ่งความรับผิดชอบ

ข้อมูลอ่อนไหว

เชื้อชาติ และเผ่าพันธ์

ความคิดเห็นทางการเมือง

ความเชื่อในลัทธิ ศาสนา หรือปรัชญา

ข้อมูลสหภาพแรงงาน

ข้อมูลพันธุกรรม

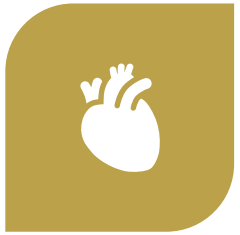
ข้อมูลชีวภาพ

ข้อมูลสุขภาพ

พฤติกรรมทางเพศ

ฐานในการประมวลผลข้อมูลอ่อนไหว

ความยินยอมโดยชัดแจ้ง



อันตรายต่อชีวิต

องค์กรไม่แสวงหากำไรเฉพาะเรื่อง

เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง

จำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย

แพทย์

สาธารณสุข

วิจัย

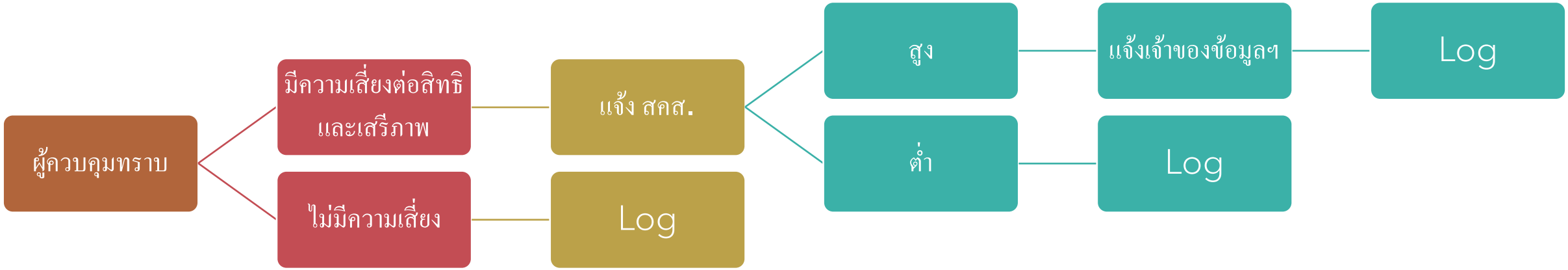
ประโยชน์สาธารณะที่สำคัญ

สิ่งที่อาจตามมา

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) – หากการประมวลผลข้อมูลอ่อนไหวเป็นกิจกรรมหลัก
- การประเมินผลกระทบของการคุ้มครองข้อมูลส่วนบุคคล (DPIA) – ในกรณีที่มีการประมวลผลที่มีความเสี่ยงสูง (High risk)
- มีโอกาสมีโทษทางอาญา

๙. หากข้อมูลรั่วไหล ไม่ต้องตกใจไป

เมื่อข้อมูลรั่วไหล



ความรับผิด

ปรับทางแพ่ง: ผู้ควบคุมและผู้ประมวลผล

- ชดเชยความเสียหาย
- เชิงลงโทษ (<2X)
- 3 ปี/10 ปี

โทษอาญา: ผู้ควบคุม

ข้อมูลอ่อนไหว

- เกิดความเสียหาย ถูกดูหมิ่นเกลียดชัง อับอาย
  - 6m/500K
- แสวงหาประโยชน์โดยมิชอบ
  - 1y/1m

โทษอาญา: ผู้ปฏิบัติหน้าที่

เปิดเผยโดยไม่ชอบ

- 6m/500K

โทษทางปกครอง

1M - 5M

ANONYMISATION

HOW TO MAKE THE DATA QUERY 'SAFE'

87%

ANONYMISATION?*

กระบวนการ

ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูล

นั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญ

*Anonymisation นั้นตรงกับคำว่า Pseudonymisation ใน GD

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

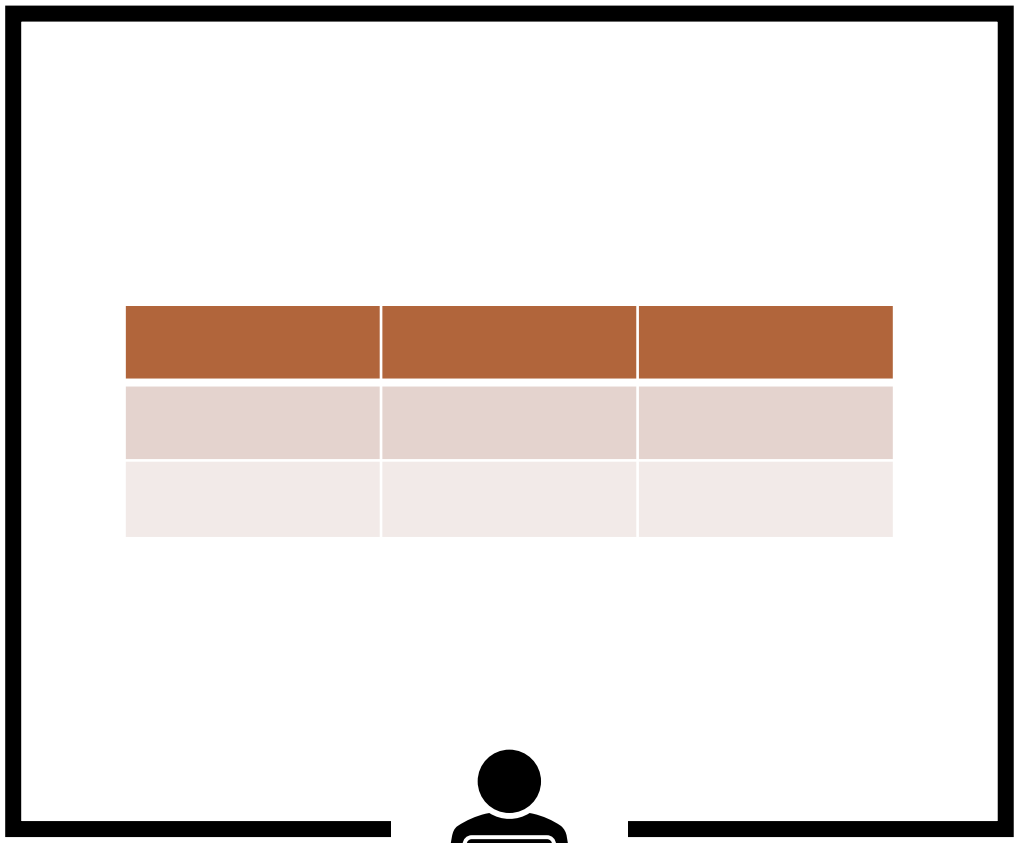
- มาตรา 37
  - (1) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี**มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป
  - (๒) ในกรณีที่ต้อง**ให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น**ที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้อง**ดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคล**โดยปราศจากอำนาจ หรือโดยมิชอบ

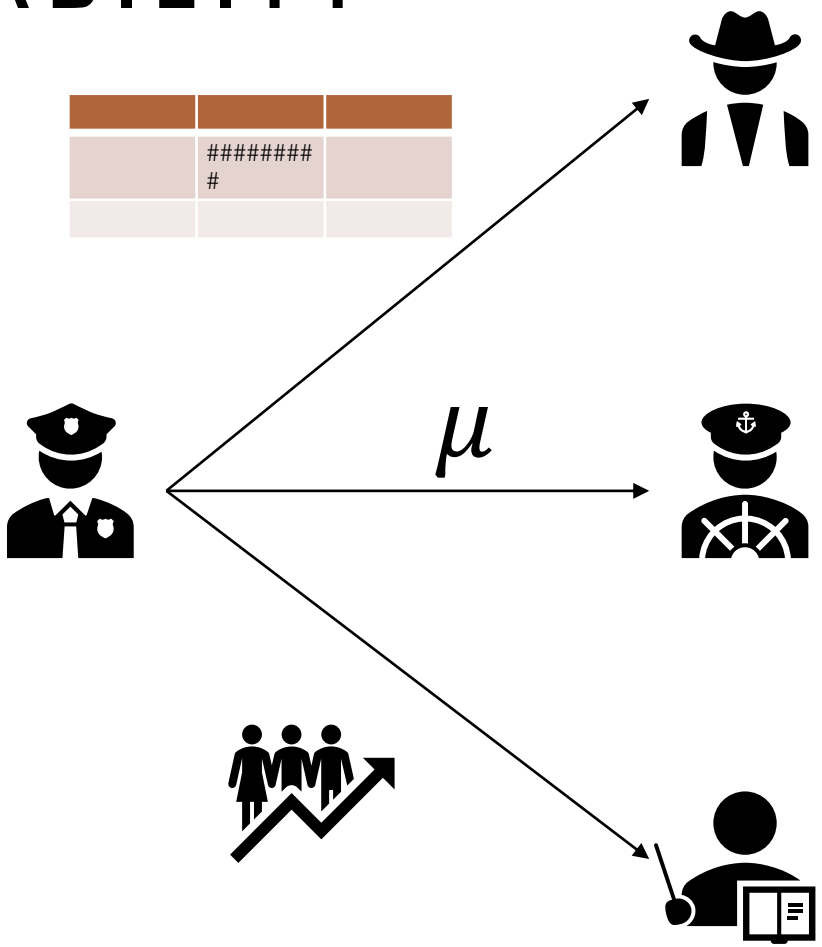
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
  - (๒) **จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล**โดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- มาตรา 4 วรรคสาม กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นการดำเนินการตามวรรคก่อน ต้องจัดให้มี**การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน**ด้วย

“SHOOT FOR THE MOON. EVEN IF YOU MISS, YOU'LL LAND AMONG THE STARS.” — NORMAN VINCENT PEALE

SECURITY = CONFIDENTIALITY + INTEGRITY + AVAILABILITY





TRADE-OFFS

Utility

- Type of analysis

Confidentiality

- Data characteristics
- Data environment

Utility 100%
Privacy 0%

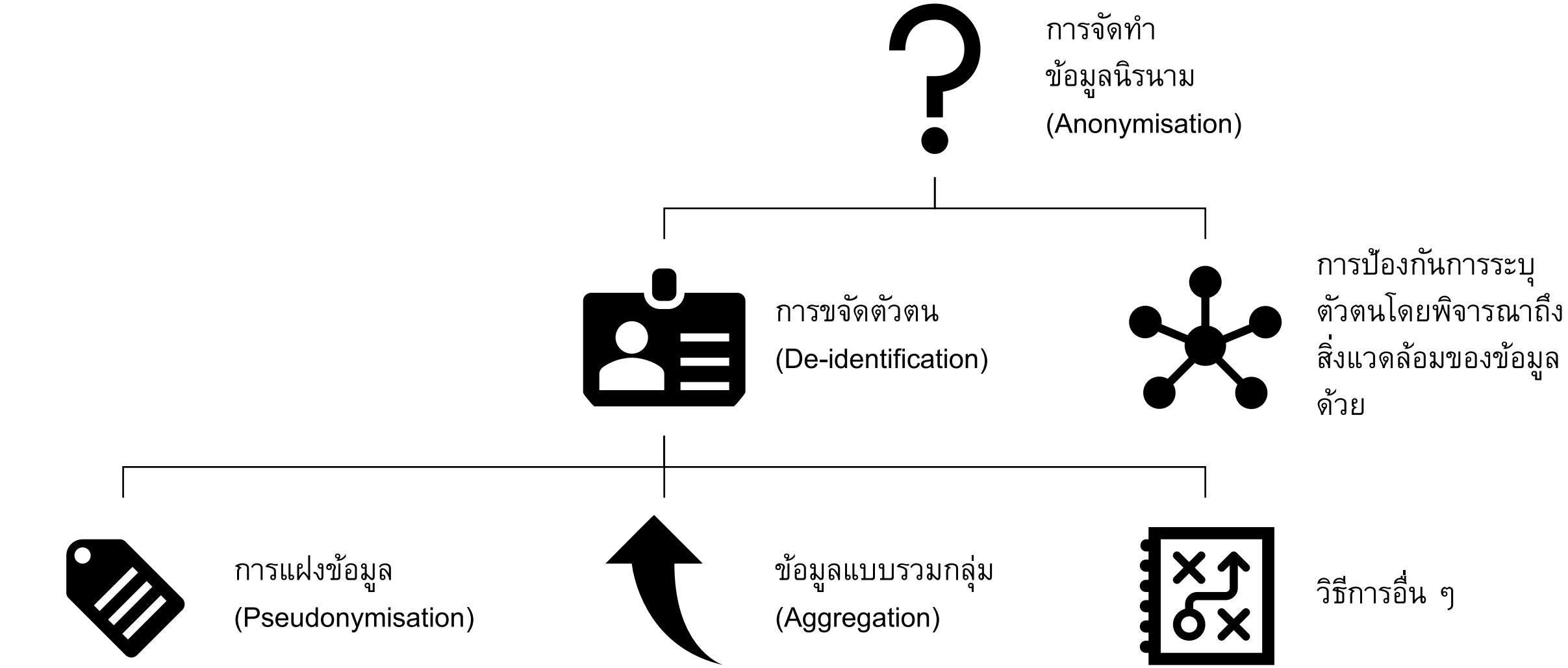
ชื่อ	วันเกิด	คะแนน
ก	7 สิงหาคม 2550	A
ข	23 มีนาคม 2550	C
ค	25 มกราคม 2551	B

Utility 0%
Privacy 100%

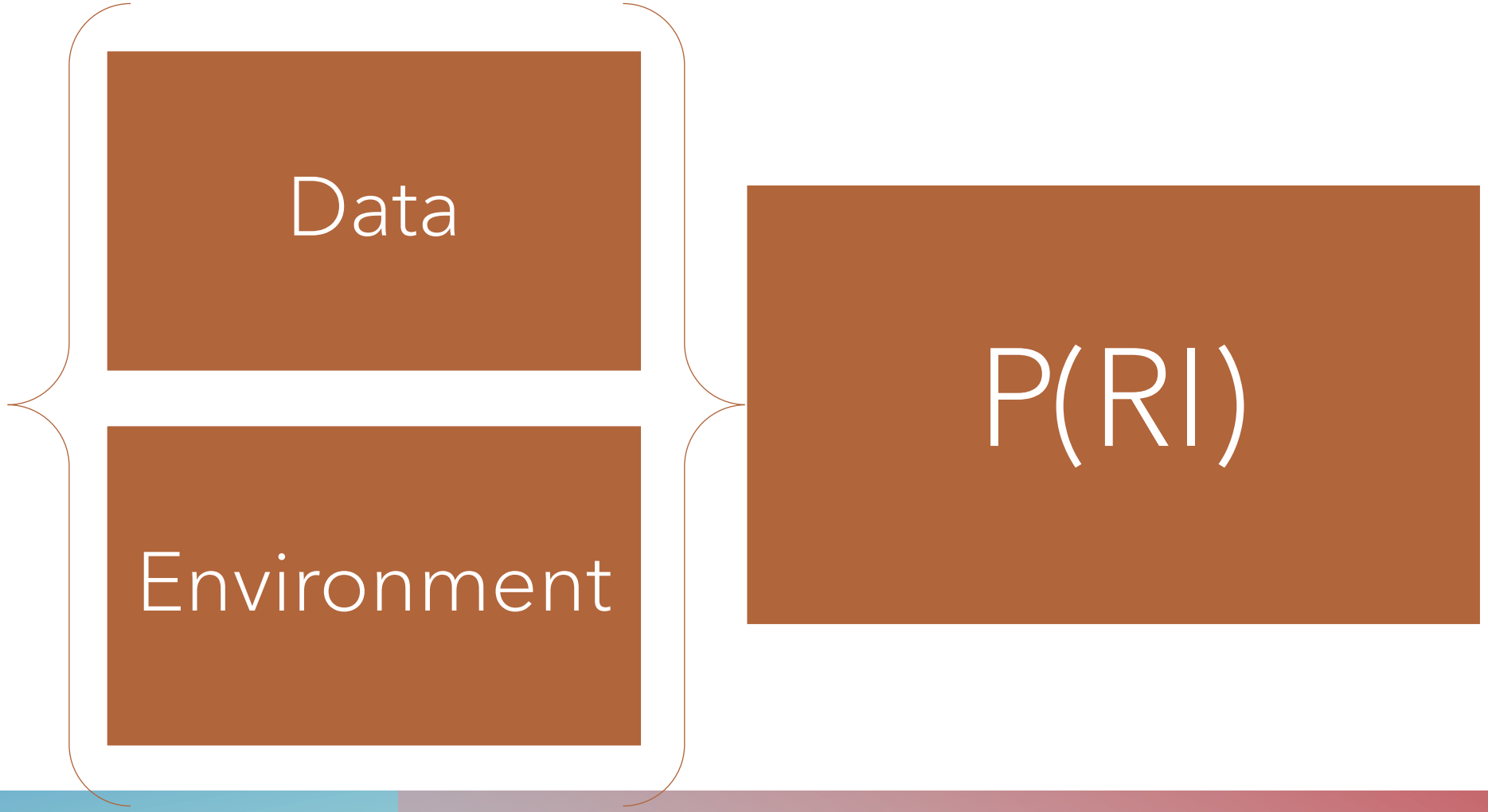
ชื่อ	วันเกิด	คะแนน
ก	-	A-C
ข	-	A-C
ค	-	A-C

Utility 50%
Privacy 50%

ชื่อ	วันเกิด	คะแนน
ก	2550	A
ข	-	-
ค	2551	B


การจัดทำ
ข้อมูลนิรนาม
(Anonymisation)
การขจัดตัวตน
(De-identification)
การป้องกันการระบุ
ตัวตนโดยพิจารณาถึง
สิ่งแวดล้อมของข้อมูล
ด้วย
การแฝงข้อมูล
(Pseudonymisation)
ข้อมูลแบบรวมกลุ่ม
(Aggregation)
วิธีการอื่น ๆ

FUNCTIONAL ANONYMISATION



ANONYMISATION FRAMEWORK

SITUATION

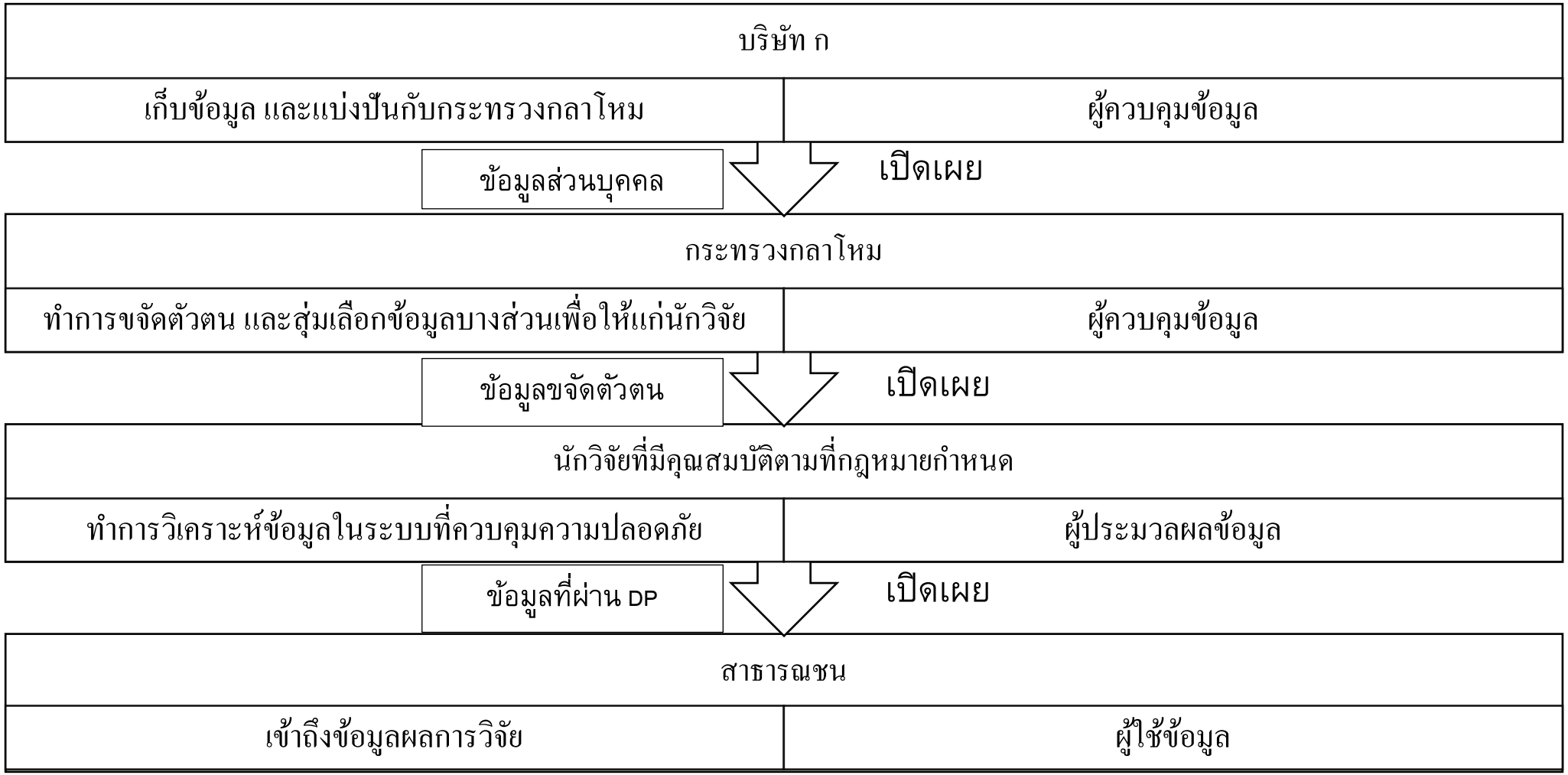
RISK

MEASURES

DATA SITUATION

QUESTION?

บริษัท ก เก็บข้อมูลของผู้ใช้บริการทั้งหมด สมมติว่ามีกฎหมายบังคับให้บริษัท ก นั้นเปิดเผยข้อมูลดังกล่าวกับกระทรวงกลาโหม เพื่อประโยชน์ในด้านความมั่นคง อย่างไรก็ตามข้อมูลดังกล่าวนั้นอาจมีประโยชน์ในด้านการวิจัย จึงมีการนำข้อมูลที่ได้ถูกลบตัวบ่งชี้ออกหมดแล้ว (de-identified data) เพื่อให้นักวิจัย ข ที่ได้รับการรับรองจากสถาบันที่กฎหมายกำหนด ใช้ภายใต้ระบบที่ป้องกันการนำข้อมูลไปใช้เกินขอบเขตของวัตถุประสงค์ในการวิจัยที่ขอไว้ล่วงหน้า หลังจากนั้นนักวิจัย ข ที่มาขออนุญาตจึงได้นำข้อมูลไปวิเคราะห์ และตีพิมพ์ผลการวิจัยเพื่อเปิดเผยต่อสาธารณชนต่อไป สถานการณ์ดังกล่าวอาจเขียนเป็นผังการเคลื่อนที่ของข้อมูลได้อย่างไร?


บริษัท ก
เก็บข้อมูล และแบ่งปันกับกระทรวงกลาโหม
ผู้ควบคุมข้อมูล
ข้อมูลส่วนบุคคล
เปิดเผย
กระทรวงกลาโหม
ทำการขจัดตัวตน และสุ่มเลือกข้อมูลบางส่วนเพื่อให้แก่นักวิจัย
ผู้ควบคุมข้อมูล
ข้อมูลขจัดตัวตน
เปิดเผย
นักวิจัยที่มีคุณสมบัติตามที่กฎหมายกำหนด
ทำการวิเคราะห์ข้อมูลในระบบที่ควบคุมความปลอดภัย
ผู้ประมวลผลข้อมูล
ข้อมูลที่ผ่าน DP
เปิดเผย
สาธารณชน
เข้าถึงข้อมูลผลการวิจัย
ผู้ใช้ข้อมูล

Data characteristics

	ความเสี่ยงต่ำ	ความเสี่ยงสูง
คุณภาพของข้อมูล	ต่ำ	สูง
อายุของข้อมูล	เก่า	ใหม่
โครงสร้างของข้อมูล	มีมิติเดียว (e.g. cross-sectional หรือ time-series)	มีหลายมิติ (e.g. longitudinal หรือ hierarchical data)
ระดับของข้อมูล	ข้อมูลรวมกลุ่ม (aggregated data)	ข้อมูลรายบุคคล หรือรายหน่วยย่อย (microdata)
ความครบถ้วนข้อมูล	ข้อมูลตัวอย่าง	ข้อมูลประชากร
ข้อมูลที่มีความอ่อนไหว	น้อย	มาก
จำนวนตัวแปรหลัก	น้อย	มาก

RISK


Strategy
Success
Growth
Strategy
Success
Growth
Business
Success
Sales
Strategy
Business
Solutions
Success
Sales
Growth
Strategy
Business

MOTIVATED INTRUDER TEST

Motivation

Ability

Access channel

Target (key) variable(s)

MOTIVATED INTRUDER TEST - TOOLS

Search engine

Public document

Prior knowledge

Similar precedents

POSSIBLE ATTACKS?

ข้อมูลที่โรงเรียนเก็บ

ชื่อ	วันเกิด	คะแนน
ก	7 สิงหาคม 2550	A
ข	23 มีนาคม 2550	C
ค	25 มกราคม 2551	B

ข้อมูลที่โรงเรียนเปิดเผย (นักเรียนรู้ชื่อลับ และวันเกิดของตน)

ชื่อ	วันเกิด	คะแนน
XX	สิงหาคม 2550	A
XY	มีนาคม 2550	C
YY	มกราคม 2551	B

หากนายหยกต้องการรู้ข้อมูล

LINKAGE ATTACK

ข้อมูลที่โรงเรียนเปิดเผย

ชื่อ	วันเกิด	คะแนน
XX	สิงหาคม 2550	A
XY	มีนาคม 2550	C
YY	มกราคม 2551	B

ข้อมูลที่นายหยก มี

ชื่อ	วันเกิด
ค	25 มกราคม 2551

POSSIBLE ATTACKS?

ข้อมูลที่โรงเรียนเก็บ

ชื่อ	วันเกิด	คะแนน
ก	7 สิงหาคม 2550	A
ข	23 สิงหาคม 2550	A
ค	25 มกราคม 2551	B

ข้อมูลที่โรงเรียนเปิดเผย (นักเรียนรู้ชื่อลับ และวันเกิดของตน)

ชื่อ	วันเกิด	คะแนน
XX	สิงหาคม 2550	A
XY	สิงหาคม 2550	A
YY	มกราคม 2551	B

หากนายหยกต้องการรู้ข้อมูล

ATRRIBUTION ATTACK

ข้อมูลที่โรงเรียนเปิดเผย

ชื่อ	วันเกิด	คะแนน
XX	สิงหาคม 2550	A
XY	สิงหาคม 2550	A
YY	มกราคม 2551	B

ข้อมูลที่นายหยก มี

รู้ว่า ข เกิดเดือนสิงหาคม

SUBTRACTION ATTACK

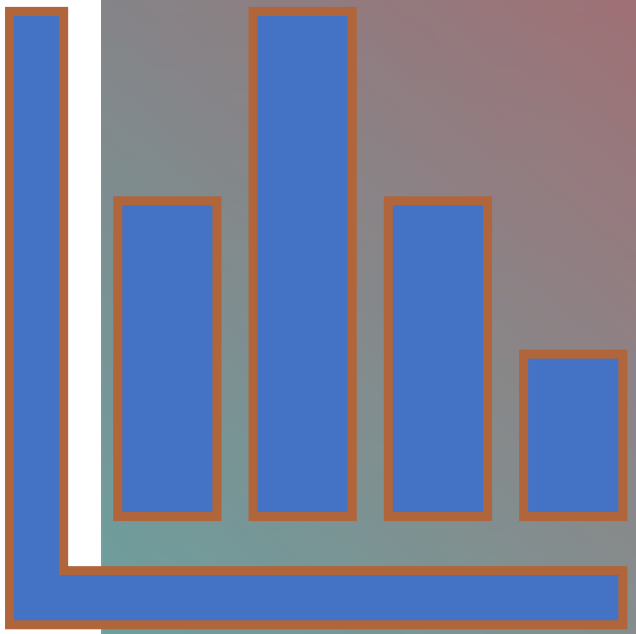
ข้อมูลที่โรงเรียนเปิดเผย

ชื่อ	วันเกิด	คะแนน
XX	สิงหาคม 2550	A
XY	สิงหาคม 2550	A
YY	มกราคม 2551	B

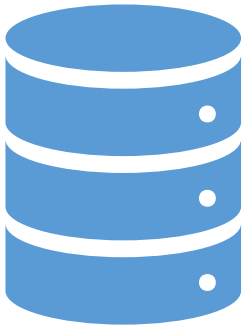
ข้อมูลที่นายหยก มี

รู้ว่าตนได้ A
รู้ว่านาย ข เกิดเดือนสิงหาคมเช่นเดียวกับตน

MEASURES



2 TYPES OF MEASURES



Data-centric approaches

Environmental approaches

DATA-CENTRIC APPROACHES

Formal

P(RI) < 1

- de-identification

Guaranteed

P(RI) → 0

- differential privacy at epsilon = 0

Statistical

0 < P(RI) < 1

- differential privacy at epsilon > 0
- Scrambing
- Masking
- Personalised
- Blurring or Noising
- Meta level

WHICH METHOD SHOULD I CHOOSE THEN?

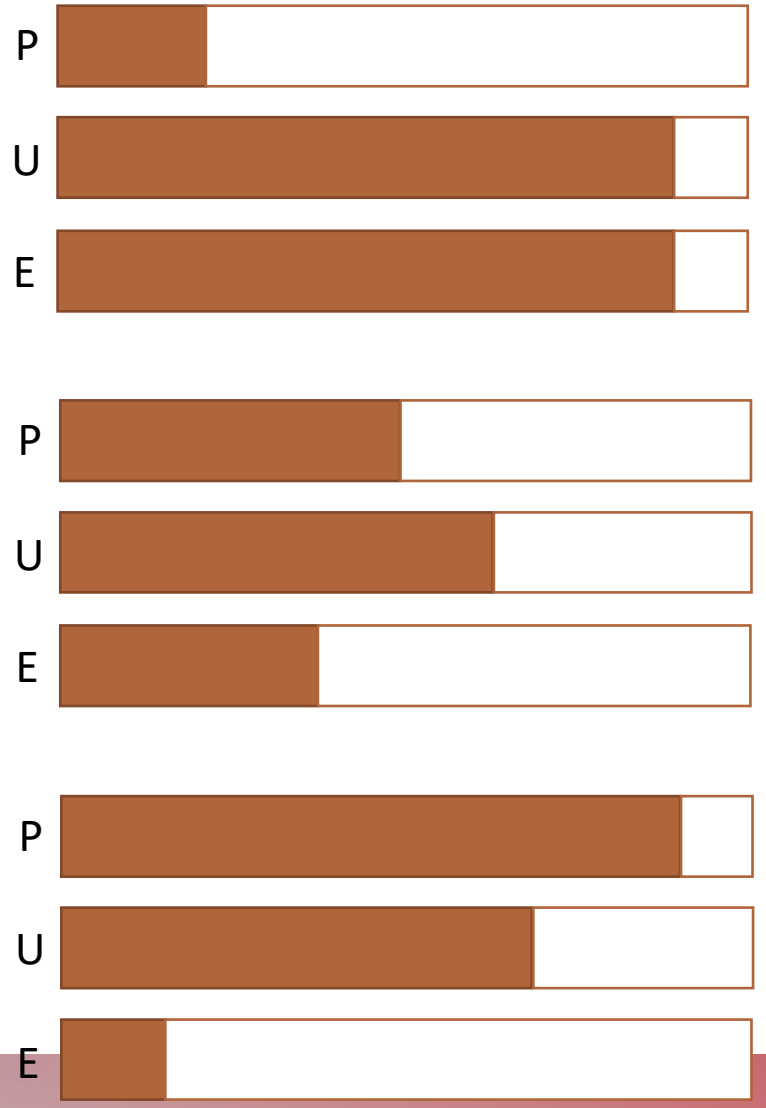
De-identification

User_id	Name	X
A00001	!@#EER	34
A00002	!e#$EW	48

K-anonymisation

User_id	Name	X
A000??	!?????	30 - 50
A000??	!?????	30 - 50

Differential privacy* $\theta + Z$



Similar method at the record level is 'synthetic' data which doesn't fall int

K-ANONYMISATION

- No combination of columns less than K rows

K-ANONYMIZATION: GENERALISATION/SUPPRESSION

ชื่อ	อายุ	เบอร์โทรศัพท์
A	30	0901234567
B	28	0919342342
C	27	0931342341
D	26	0943123213

K = 2

ชื่อ	อายุ	เบอร์โทรศัพท์
X	27-28	09XXXXXXXX
X	27-28	09XXXXXXXX
X	26-27	09XXXXXXXX
X	26-27	09XXXXXXXX

K = ?

Identify & Evaluate 2 Risk Factors

Determine "preferences"

Calculate K as %

ε-DIFFERENTIAL PRIVACY

GDPR compliant
Pseudonymisation
requires separation of the
information value of data
from the means of linking
the data to individuals.*

*https://www.trustarc.com/blog/2017/07/17/can-legally-analytics-gdpr/#_ft

ε-DIFFERENTIAL PRIVACY: WHAT DOES IT PROMISE?

"I'll learn as much as possible about a group and as little as possible about an individual"

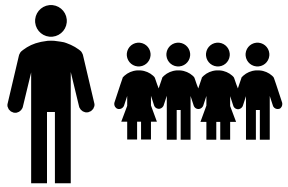
*https://www.trustarc.com/blog/2017/07/17/can-legally-analytics-gdpr/#_ft

2 KEY PROPERTIES OF ε-DIFFERENTIAL PRIVACY

Post-processing invariance

Composition

ε-DIFFERENTIAL PRIVACY

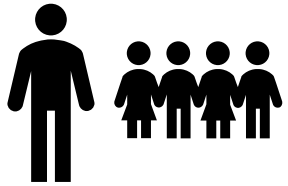


$\overline{Height_1}$

$\overline{Height_2}$

No difference more than the degree of ε

$\mathcal{E}$-DIFFERENTIAL PRIVACY

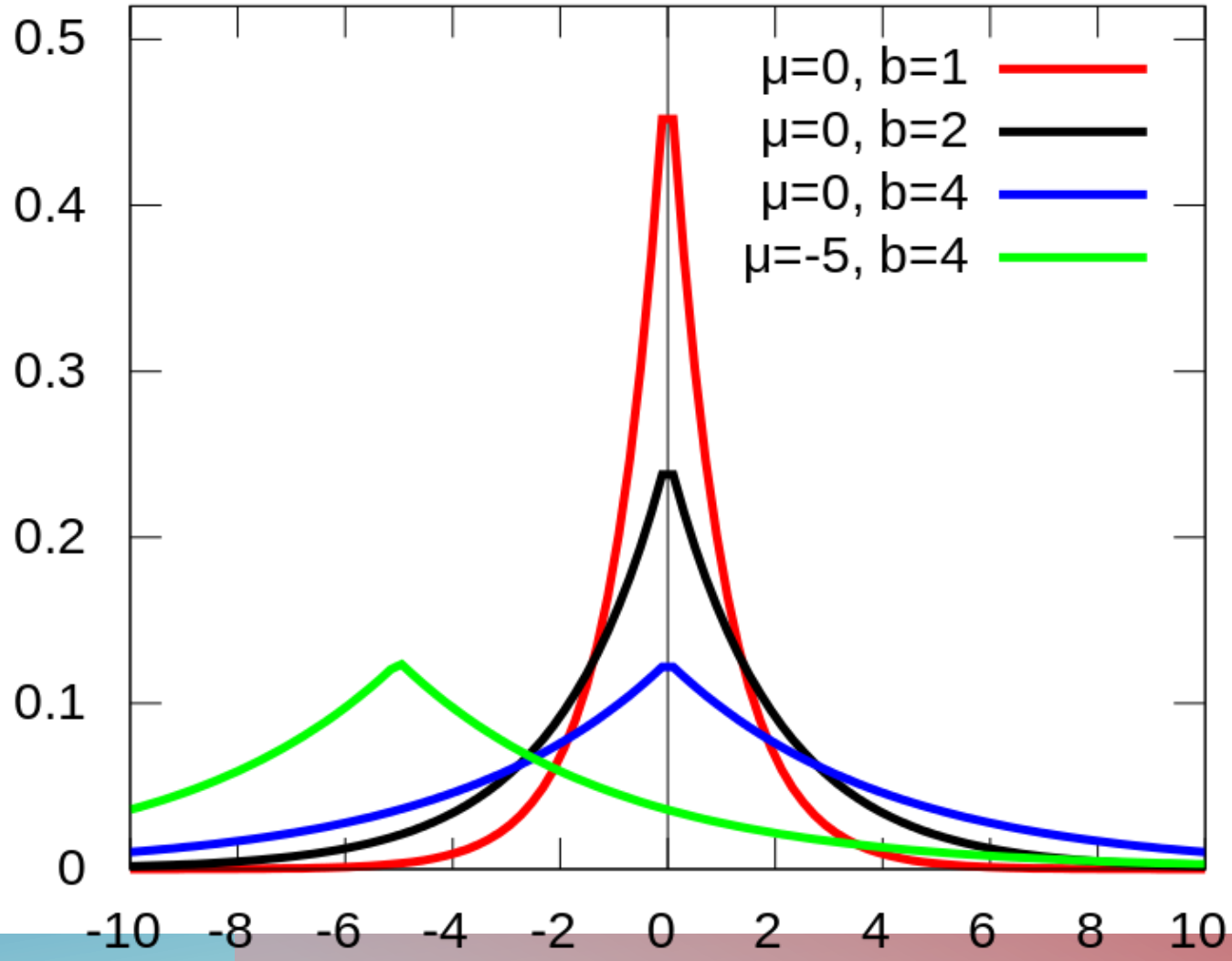


$\overline{Height_1} + Z \sim \theta(\varepsilon)$

$\overline{Height_2} + Z \sim \theta(\varepsilon)$

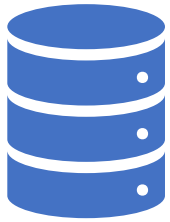
No difference more than the degree of ε

ε-DIFFERENTIALLY LAPLACE PRIVACY



$b = 1/\varepsilon$

WHERE TO DO DIFFERENTIAL PRIVACY?

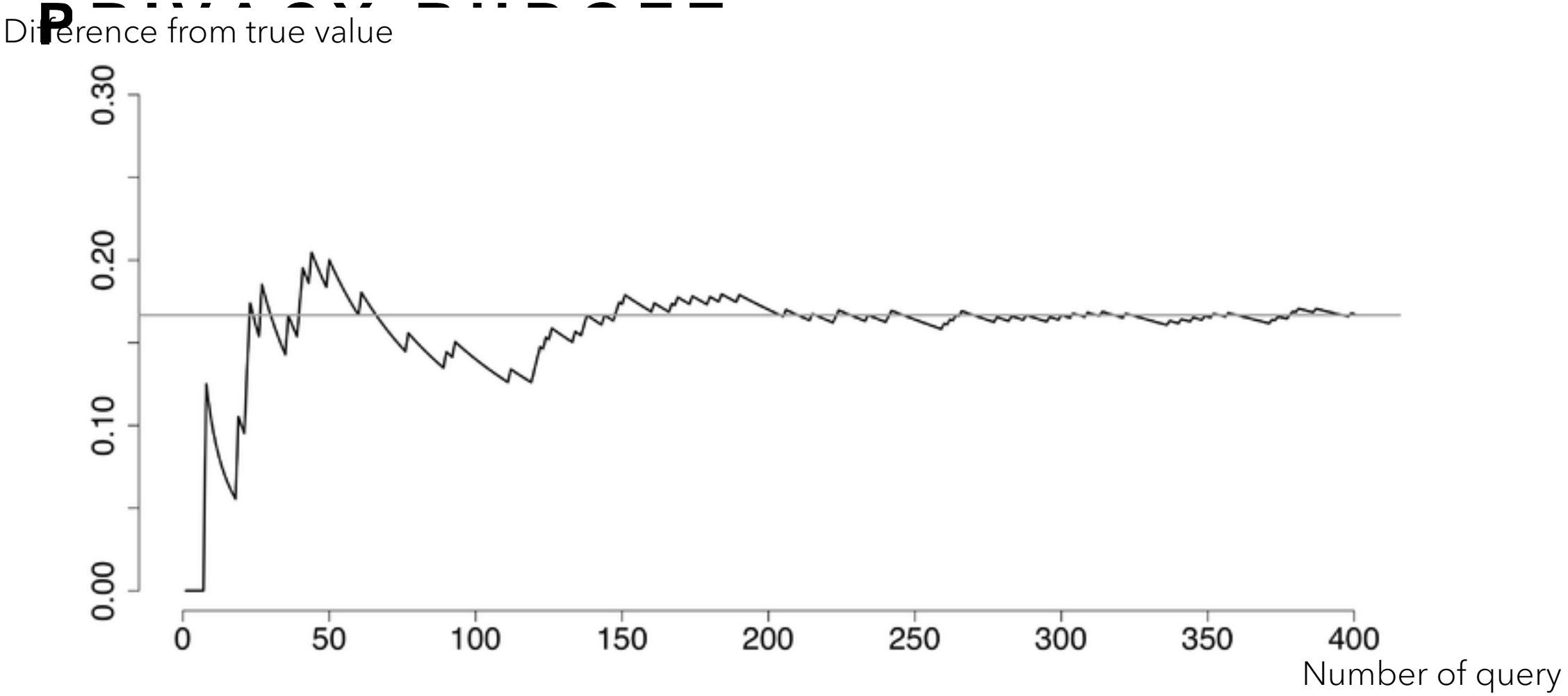


Data

Analysis

Disclose

PRIVACY BUDGET



ความเสี่ยงของการเปิดเผยข้อมูล	ประโยชน์สาธารณะในการใช้ข้อมูล	ค่า ε ที่เหมาะสม	Privacy budget
สูง	สูง	0.001 – 0.01	ต่ำ
สูง	ต่ำ	0.01 – 0.1	ปานกลาง
ต่ำ	สูง	0.01 – 0.1	ปานกลาง
ต่ำ	ต่ำ	0.1 – 1.0	สูง

ENVIRONMENTAL APPROACHES

Accessed person

Relationship with organization

Certificate or Guarantee

Scope of analysis

Mode of access

Open

Deliver

On-site or Virtual

License

Data situation

- Data flowchart
- Controller/processor?
- Data characteristics
- All principles applied (legality, consent, etc.)

Risk

- Data evaluation
- Tests
  - Motivated intruder test
  - Precedent comparison
- Possible attacks
  - Linkage
  - Attribution
  - Subtraction
  - Etc.

Measures

- Change data
  - Meta-level > Micro-level
  - Aggregation
  - Drop
  - Sampling
  - Distortion
  - Differential privacy***
- Change environment
  - Who can access?
  - What analysis?
  - Mode of access?

SOME EXAMPLES

TRACKING JOURNEY BY MOBILE DATA

Mobile Phone Number	DoB	Journey time	Location	Date and Time
0893431235	01/09/1989	17m 23s	Lumphini, Bangkok	7/8/2019 14:12:14
0987938492	30/10/1978	23m 14s	LadPhrao, Bangkok	3/9/2019 09:34:25
0983749384	12/12/1968	13m 15s	Muang, Samut Prakan	8/10/2019 23:34:12

TRACKING JOURNEY BY MOBILE DATA: SOME POSSIBLE ANONYMISATION

Hashed ref. no.	Age band	Journey time	Location	Date and Time
1340X23CS	30 - 40	17m	Bangkok	Aug2019 afternoon
403253SK23	40 - 50	23m	Bangkok	Sep2019 morning
8923KOX091	50 - 60	13m	Samut Prakan	Oct2019 night

All in all, it depends on the 'purpose' of your data processing
Marginal confidentiality should not exceed marginal utility.

THIRD PARTIES' PRIOR KNOWLEDGE CASE

- HR employees record
  - Name: P Chalahedchala
  - DoB: 01/01/1999
  - Sex: M
  - Address 145/99 Rachaprapakarn Rd., Bangkok, 10420
  - Start date: 11/06/2017
- Anonymised research database extract
  - Age: 20
  - Sex: M
  - Post Code: 10420
  - Period of Service: 3 years
  - HIV: Positive

THIRD PARTIES' PRIOR KNOWLEDGE

CASE

- HR employees record
  - Name: P Chalahedchala
  - DoB: 01/01/1999
  - Sex: M
  - Address 145/99 Rachaprapakarn Rd., Bangkok, 10420
  - Start date: 11/06/2017
- (Blurred) anonymised research database extract
  - Age rage: 20-30
  - Sex: M
  - Location: Bangkok
  - Period of Service: 1-5 years
  - HIV: Positive

THIRD PARTIES' PRIOR KNOWLEDGE CASE

- HR employees record
  - Name: P Chalahedchala
  - DoB: 01/01/1999
  - Sex: M
  - Address 145/99 Rachaprapakarn Rd., Bangkok, 10420
  - Start date: 11/06/2017
- (Blurred + Meta-level) anonymised research database extract
  - "In Bangkok branch, 3% of male employees with 1– 5 years' service have contracted HIV.

ภาครัฐ

การโอนข้อมูลระหว่างหน่วยงาน

- พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - มาตรา ๓ ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมาย ว่าด้วยการนั้น เว้นแต่
    - (๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Legal bases and security) และบทบัญญัติ เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data subject rights) รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติ แห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม
- พรบ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540
  - มาตรา ๒๔ หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานรัฐแห่งอื่น หรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้
    - (๒) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น
    - (๓) ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

การโอนข้อมูลระหว่างหน่วยงาน

- Simpler version: เปิดเผยระหว่างหน่วยงานของรัฐได้ แต่ต้องหา Legal basis และให้สิทธิแก่เจ้าของข้อมูลตามที่เหมาะสม
- ในกฎหมายทั้งสองฉบับไม่ได้ให้ขอความยินยอม (พรบ. ข้อมูลข่าวสารฯ บอกว่าแชร์ได้ไม่ต้องขอความยินยอม ตาม ม. 24 (3) ส่วน พรบ. ข้อมูลส่วนบุคคลฯ บอกว่าถ้าหาฐานทางกฎหมายได้ก็โอเค ซึ่งก็เข้า public task กับ legal obligation ทั้งผู้รับและผู้ให้ข้อมูล จึงไม่ต้องขอความยินยอม (อาจเพียงแค่แจ้ง) โดยที่ พรบ. สถิติก็บอกว่าให้ anonymise ด้วยในการส่งมาเท่านั้นเอง) ดังนั้น ก็แชร์ข้อมูลได้เลยเพียงเท่าที่จะบรรลุวัตถุประสงค์นั้นๆ

PUBLIC TASKS FIRST. CONSENT LAST.

- พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - มาตรา 24 (4) เป็น**การจำเป็น**เพื่อการปฏิบัติหน้าที่**ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ**ของผู้ควบคุมข้อมูลส่วนบุคคล หรือ**ปฏิบัติหน้าที่ในการใช้อำนาจรัฐ**ที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

พรบ. สถิติ พ.ศ. 2550: อำนาจหน้าที่ (ม. ๖)

- (๔) จัดทำสำมะโนหรือสำรวจตัวอย่าง...
- (๗) ประสานกับหน่วยงานในการสร้างเครือข่ายสถิติ เพื่อให้ได้มาซึ่งฐานข้อมูลสถิติที่สำคัญและเป็นปัจจุบันของประเทศ
- (๘) ให้บริการสถิติ...
- (๙) เผยแพร่สถิติ...
- (๑๑) ปฏิบัติการอื่นๆ

พรบ. สถิติ พ.ศ. 2550: อำนาจหน้าที่ (ม. ๙. ๑๐. ๑๑)

- กำหนดให้เป็นหน้าที่ของประชาชนที่จะต้องให้ข้อมูล ให้กำหนดโดยกฎกระทรวง และมีสาระสำคัญ เช่น วัตถุประสงค์ ระยะเวลา เขตท้องที่ ฯลฯ
- รายละเอียดการดำเนินงานตามประกาศโดย ผ.อ.
- คนที่ถูกระบุมีหน้าที่ตามกฎหมาย (Legal obligation)

พรบ. สถิติ พ.ศ. 2550: ความร่วมมือจากหน่วยงาน (ม. ๔ และ ๑๔)

- มาตรา ๔ “หน่วยงาน หมายความว่า ส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรปกครองส่วนท้องถิ่น และหน่วยงานอื่นของรัฐ”
- มาตรา ๑๔ หน่วยงานมีหน้าที่ต้องให้ความร่วมมือ หากข้อมูลนั้นจำเป็นในการจัดสร้างเครือข่ายสถิติ และพัฒนาฐานข้อมูลที่สำคัญและเป็นปัจจุบันของประเทศ (legal obligation)
  - หน่วยงานต้องส่งให้ภายใน 30 วันนับแต่ได้รับแจ้ง
  - ต้องไม่ระบุหรือเปิดเผยว่าเป็นข้อมูลของบุคคลใด (anonymized data)
    - เว้นแต่ ยินยอม หรือเปิดเผยต่อสาธารณะอยู่แล้ว

พรบ. สถิติ พ.ศ. 2550: เปิดเผยได้จำกัด (ม. ๑๕)

- เก็บเป็นความลับ เว้นแต่
  - สอบสวนพิจารณคดีตาม พรบ. นี้
  - เปิดเผยต่อหน่วยงานเพื่อประโยชน์ในการจัดทำสถิติ วิเคราะห์หรือวิจัย ทั้งนี้เท่าที่ไม่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล และต้องไม่ระบุหรือเปิดเผยถึงเจ้าของข้อมูล

BUT YOU MAY REJECT…

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐ หรือหน้าที่ตามกฎหมาย	ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1.การเพิกถอนความยินยอม	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
4.การลบข้อมูลส่วนบุคคล	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗
5.การระงับการประมวลผลข้อมูล [162]	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

Source: Thailand Data Protection Guideline

สิ่งที่พึงทำเป็นอย่างน้อยเมื่อใช้ฐานภารกิจรัฐ

Privacy notice (per reference to privacy policy)

Find the ‘statutory basis’ if possible

Processing agreements

Security remains

บางวัตถุประสงค์อาจต้องใช้ฐานอื่น

- คุกกี้เว็บไซท์
- CCTV
- ฝ่ายบุคคล
- การดำเนินการอื่นๆ

ข อ บ คุ ณ ค รั บ

- พีรพัฒ โชคสุวัฒนสกุล
- peerapat.chokesuwattanskul@gmail.com