PDPA Implementation Guidelines Seminar

สัมมนาให้ความรู้เกี่ยวกับแนวทางการปฏิบัติตาม
กฎหมายคุ้มครองข้อมูลส่วนบุคคล

โดย
บริษัท เอเทนติค คอนซัลติ้ง จำกัด
18 มีนาคม พ.ศ. 2565

ATHENTIC CONSULTING

สมาคมบริษัทหลักทรัพย์ไทย ASCO
ASSOCIATION OF THAI SECURITIES COMPANIES

ATHENTIC CONSULTING
THE TRUE REGTECH EXPERT

Table of contents

ความสำคัญและวัตถุประสงค์ของ PDPA

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่มุ่งวางหลักเกณฑ์การสร้างมาตรฐานการคุ้มครองความเป็นส่วนตัวของบุคคลให้เทียบเท่านานาประเทศ โดยวางกรอบสิทธิหน้าที่ของทั้งหน่วยงานรัฐ หน่วยงานเอกชน และภาคประชาชน เพื่อรักษาสมดุลระหว่างการใช้ข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว พร้อมมาตรฐานความปลอดภัยของการใช้ข้อมูลส่วนบุคคล

บุคคลที่เกี่ยวข้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

Data Subjects

เจ้าของข้อมูลส่วนบุคคล
คือ ผู้ที่ถูกข้อมูลชี้ไป/ระบุตัว

Data Controller

ผู้ควบคุมข้อมูล
คือ ผู้กำหนดวัตถุประสงค์ใน
การเก็บ ใช้ เปิดเผยข้อมูล

Data Processor

ผู้ประมวลผลข้อมูล
คือ ผู้ประมวลผลข้อมูลตาม
คำสั่งของผู้ควบคุมข้อมูล

ATHENTIC CONSULTING
Truly Regtech Expert

บุคคลที่เกี่ยวข้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

Data Subjects

พนักงาน
ลูกค้า
คู่สัญญา

Data Controller

บริษัทหลักทรัพย์

บริษัทพาร์ทเนอร์

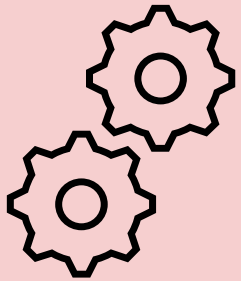
Data Processor

บริษัทคู่ค้า

เช่น Payroll System, HR System, IT

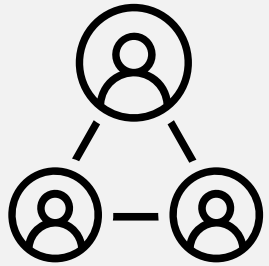
ATHENTIC CONSULTING
Truly Regtech Expert

บทบาทหน้าที่ของผู้ควบคุมข้อมูล



จัดให้มีมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการ

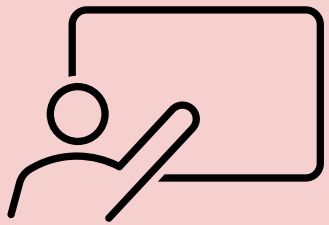
การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล



แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

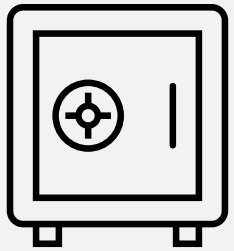
จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

บทบาทหน้าที่ของผู้ประมวลผลข้อมูล



ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูล

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล



จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูล

จัดทำและเก็บรักษารายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

มีความชอบด้วยกฎหมาย

อธิบายได้ว่านำข้อมูลไปใช้เพื่อวัตถุประสงค์อะไร

มีมาตรการคุ้มครองข้อมูล

มาตรการในการดูแลความปลอดภัย
รวมถึงมาตรการในการแก้ไขเยียวยา

ATHENTIC CONSULTING
Truly Regtech Expert

PDPA Checklist

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ (มาตรา 28,29)

สัญญาการประมวลผลข้อมูลส่วนบุคคล (มาตรา 40)

ช่องทางการใช้สิทธิของเจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

ATHENTIC CONSULTING
Truly Regtech Expert

บทบาทและหน้าที่ของ DPO

ให้คำแนะนำและตรวจสอบ
การดำเนินงานภายใน
องค์กรให้เป็นไปตามพรบ.

ให้ความร่วมมือกับ
สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

รักษาความลับที่ได้มาจาก
การทำหน้าที่

ได้รับความคุ้มครอง
เพื่อให้มีความเป็นอิสระในการปฏิบัติหน้าที่

ATHENTIC
CONSULTING
Truly Regtech Expert

PDPA Checklist

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ (มาตรา 28,29)

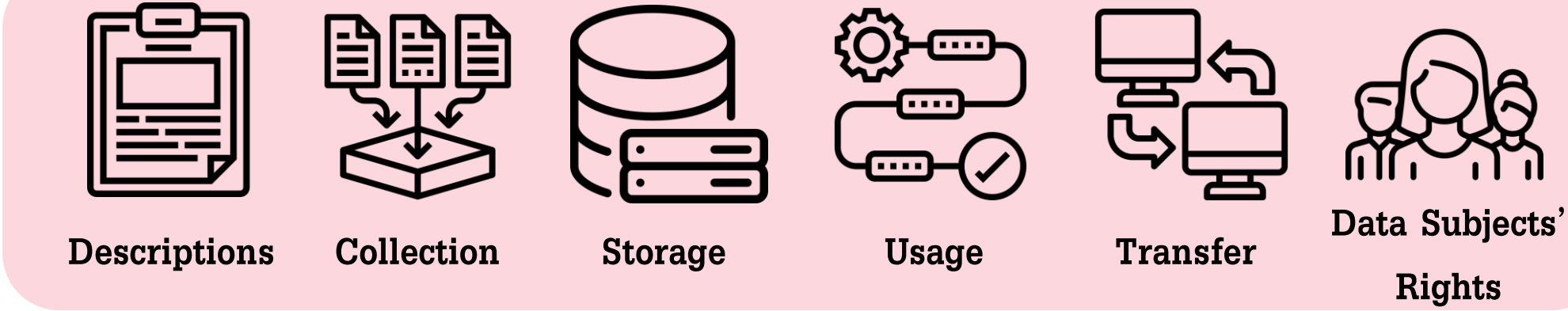
สัญญาการประมวลผลข้อมูลส่วนบุคคล (มาตรา 40)

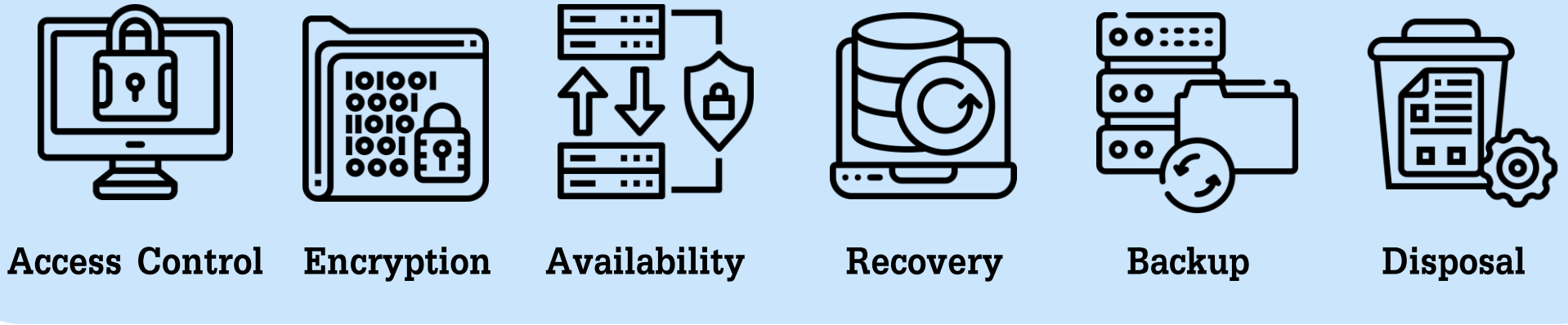
ช่องทางการใช้สิทธิของเจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

ATHENTIC CONSULTING
Truly Regtech Expert

Records of Processing Activities





ATHENTIC CONSULTING
Truly Regtech Expert

ฐานการประมวลผลข้อมูลส่วนบุคคล (มาตรา 24)

สัญญา
(Contract)

หน้าที่ตามกฎหมาย
(Legal Obligations)

ภารกิจรัฐ
(Public Task)
มักใช้สำหรับหน่วยงานรัฐ

ประโยชน์ต่อชีวิต ร่างกาย อนามัย
(Vital Interest)

ประโยชน์อันชอบธรรม
(Legitimate Interest)

ความยินยอม
(Consent)

การวิจัย สถิติ และเอกสารทางประวัติศาสตร์

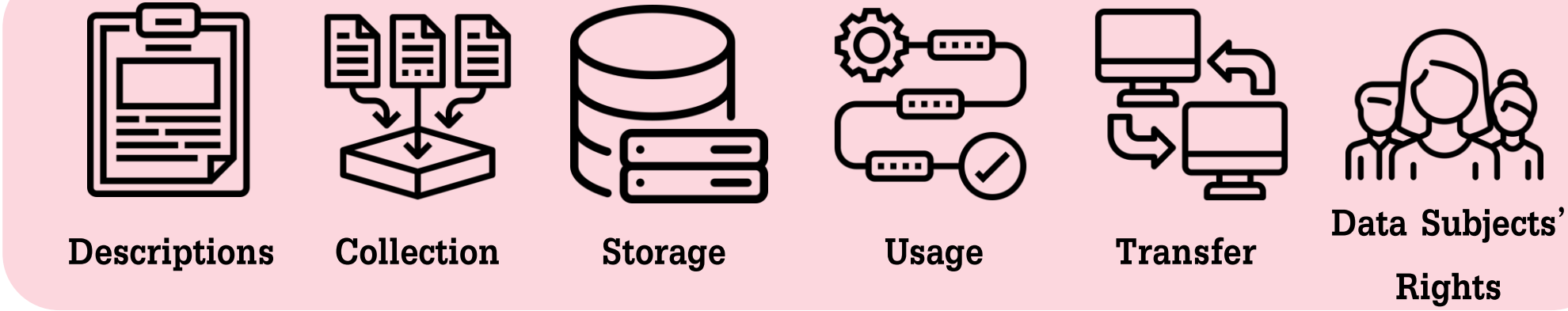
ATHENTIC
CONSULTING
Truly Regtech Expert

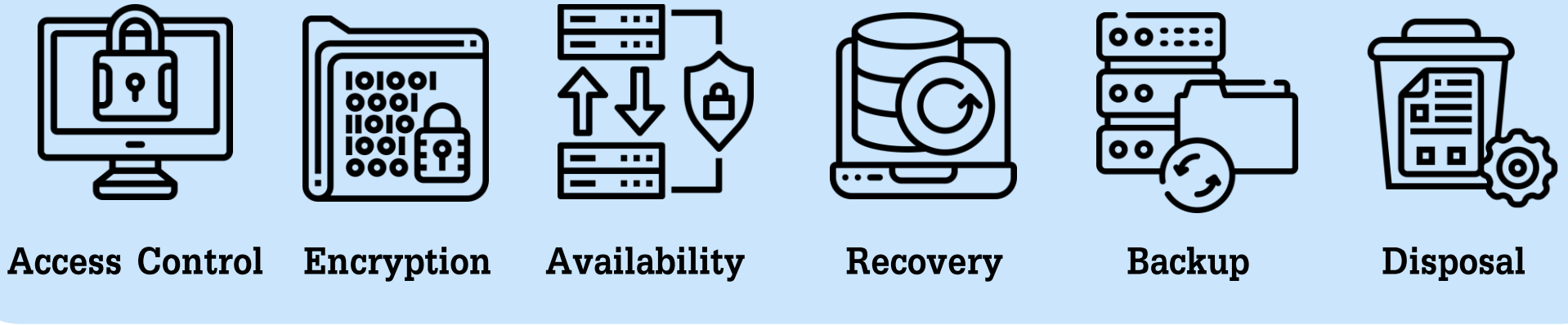
ฐานและกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับบริษัทหลักทรัพย์

สัญญา (Contract)	กิจกรรมที่เกี่ยวข้องกับกระบวนการเสนอขายหลักทรัพย์ รูปแบบการให้บริการซึ่งอยู่ในลักษณะของสัญญาว่าจ้างที่ปรึกษาทางการเงิน
หน้าที่ตามกฎหมาย (Legal Obligations)	การเปิดเผยข้อมูลตามที่กฎหมายกำหนด เช่น ประกาศของสำนักงาน ก.ล.ต., ข้อบังคับของตลาดหลักทรัพย์ที่ออกตาม พ.ร.บ.หลักทรัพย์
ประโยชน์อันชอบธรรม (Legitimate Interest)	การเก็บข้อมูลการดำเนินงานเพื่อใช้เป็นข้อต่อสู้ทางกฎหมาย
ความยินยอม (Consent)	การทำการตลาดทางตรง

ATHENTIC CONSULTING
Truly Regtech Expert

Records of Processing Activities





ATHENTIC CONSULTING
Truly Regtech Expert

การจัดการความเสี่ยง

ความเสี่ยง	ตัวอย่าง	ผลกระทบและการแก้ไข
 High	• ข้อมูลอ่อนไหว เช่น ลายนิ้วมือ ม่านตา	• ผลกระทบร้ายแรง • แก้ไขด้วยต้นทุนสูง
Moderate	• ชื่อสกุล รหัสประจำตัวเลขบัตรประชาชน	• ผลกระทบสามารถแก้ไขได้ด้วยต้นทุนปานกลาง
 Low	• เบอร์โทรศัพท์	• ผลกระทบสามารถแก้ไขได้ด้วยต้นทุนต่ำ

การประเมินความเสี่ยง

1. การระบุตัวบุคคล
2. ปริมาณข้อมูล
3. การควบคุมการเข้าถึง
4. ผลกระทบต่อเจ้าของข้อมูล
5. ผลกระทบต่อองค์กร

ATHENTIC CONSULTING
Truly Regtech Expert

PDPA Checklist

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ (มาตรา 28,29)

สัญญาการประมวลผลข้อมูลส่วนบุคคล (มาตรา 40)

ช่องทางการใช้สิทธิของเจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

ATHENTIC CONSULTING
Truly Regtech Expert

หน้าที่ในการแจ้ง

(Privacy Policy and Notices)

วัตถุประสงค์ และ
ฐานการประมวลผล

ประเภทของข้อมูล

ระยะเวลา
การจัดเก็บข้อมูล

การโอนข้อมูล

การรักษาความ
ปลอดภัยของข้อมูล

สิทธิของ
เจ้าของข้อมูล

ข้อมูลการติดต่อ
ผู้ควบคุมข้อมูล

ATHENTIC
CONSULTING
Truly Regtech Expert

PDPA Checklist

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ (มาตรา 28,29)

สัญญาการประมวลผลข้อมูลส่วนบุคคล (มาตรา 40)

ช่องทางการใช้สิทธิของเจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

ATHENTIC CONSULTING
Truly Regtech Expert

สิทธิของเจ้าของข้อมูล

1. สิทธิในการถอนความยินยอม
2. สิทธิในการได้รับแจ้งข้อมูล
3. สิทธิในการเข้าถึงข้อมูล
4. สิทธิในการแก้ไขข้อมูล
5. สิทธิในการลบข้อมูล
6. สิทธิในการระงับการประมวลผล
7. สิทธิในการโอนข้อมูล
8. สิทธิในการคัดค้านการประมวลผล
9. สิทธิเกี่ยวกับการประมวลผลอัตโนมัติ

เหตุปฏิเสธ

- ใช้สิทธิโดยมิชอบหรือจงใจทำให้เกิดความวุ่นวาย
- ใช้สิทธิเกินส่วน

ATHENTIC CONSULTING
Truly Regtech Expert

PDPA Checklist

นโยบายโดยผู้บริหาร (มาตรา 81)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (มาตรา 41)

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (มาตรา 39)

การแจ้งเจ้าของข้อมูล (มาตรา 23,25)

การขอความยินยอม (มาตรา 19)

การส่งต่อ/โอนข้อมูลไปยังต่างประเทศ (มาตรา 28,29)

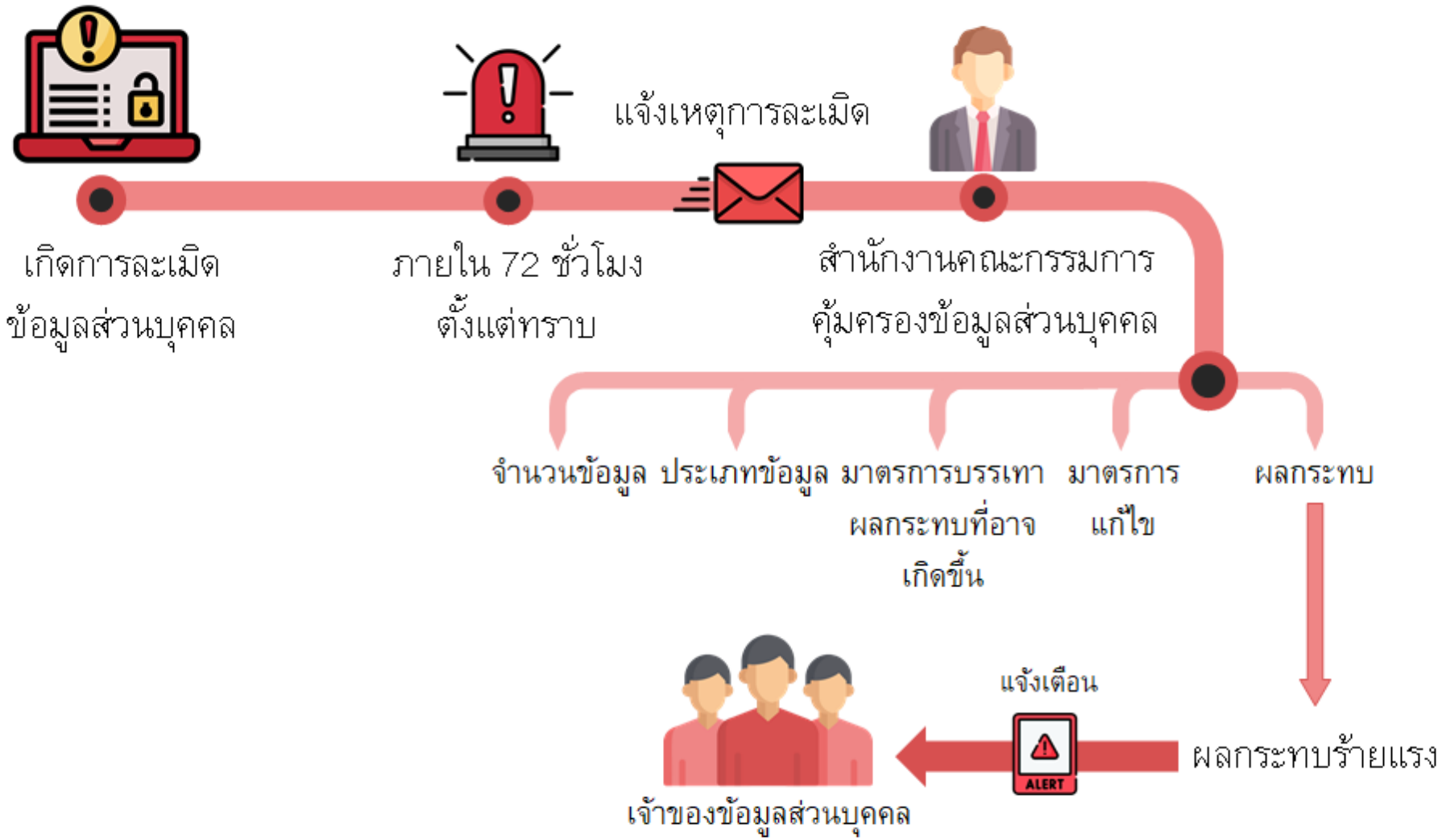
สัญญาการประมวลผลข้อมูลส่วนบุคคล (มาตรา 40)

ช่องทางการใช้สิทธิของเจ้าของข้อมูล (มาตรา 30-36)

การแจ้งเหตุละเมิด (มาตรา 37)

ATHENTIC CONSULTING
Truly Regtech Expert

Data Breach Notification



Icons made by https://www.flaticon.com/authors

ATHENTIC CONSULTING
Truly Regtech Expert

บทลงโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษอาญา

สูงสุดจำคุก**ไม่เกิน 1 ปี**

ปรับ**ไม่เกิน 1,000,000 บาท**

โทษทางปกครอง

สูงสุดปรับ**ไม่เกิน 5,000,000 บาท**

ความรับผิดทางแพ่ง

ค่าเสียหาย และ

ค่าสินไหมเชิงลงโทษ 2 เท่า