



**“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**  
**กับการเชื่อมโยงแลกเปลี่ยนและการใช้ประโยชน์ข้อมูลผู้ป่วย”**

**สำหรับ สำนักงานปลัดกระทรวงสาธารณสุข**

**รุ่นที่ 1 วันที่ 19 สิงหาคม 2562**

**รุ่นที่ 2 วันที่ 22 สิงหาคม 2562**

**รุ่นที่ 3 วันที่ 26 สิงหาคม 2562**

**สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม**

# About Speaker

จักรพงษ์ ชางษ์

**Jakkrapong Chavong**

Executive Director

**Office of The Permanent Secretary**

Ministry of Digital Economy and Society

## Current Assignment Related to Data Protection / Privacy



เป็นผู้แทนประเทศไทยในส่วนของกระทรวงฯ

- เข้าร่วมการเจรจาคณะทำงานด้านพาณิชย์อิเล็กทรอนิกส์ (RCEP WGEC) ภายใต้การประชุมคณะกรรมการเจรจาการค้า Regional Comprehensive Economic Partnership (RCEP) ตั้งแต่ปี 2558 จนถึงปัจจุบัน
- เข้าร่วมการเจรจาเตรียมการ FTA TH-EU, CPTPP, JTEPTA ในด้านพาณิชย์อิเล็กทรอนิกส์



ร่วมในการศึกษา วิเคราะห์ พิจารณาและดำเนินการปรับแก้ไขร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และปรับปรุงแก้ไขเป็นฉบับกระทรวงฯ กุมภาพันธ์ 2561



ร่วมในการพิจารณาและปรับปรุงแก้ไขร่างในชั้นกฤษฎีกาและผ่าน สนช.



เป็นผู้แทนไทยเข้าร่วมประชุมคณะทำงาน ASEAN Framework on Digital Data Governance ปี 2561-2562

เป็นผู้แทนไทยเข้าร่วมประชุม APEC Cross-Border Privacy Rules System ฯ ปี 2561

เป็นวิทยากรบรรยาย PDPA ให้หน่วยงานภาครัฐ และ PDPA Compliance ให้หน่วยงานภาคเอกชน



# Agenda

## 1 – สารสำคัญของ PDPA

- 1.1 หลักการสำคัญ และขอบเขตการบังคับใช้
- 1.2 สิทธิและหน้าที่ของผู้ที่เกี่ยวข้อง  
(Data controller, Data Processor)
- 1.3 การเก็บข้อมูล การใช้ การเปิดเผยข้อมูล

## 2 – การเชื่อมโยงแลกเปลี่ยนและ การใช้ประโยชน์ข้อมูลผู้ป่วย

## 3 – แนวทางการปฏิบัติตาม PDPA

## 4 – Q&A





## สาระสำคัญของ PDPA





พระราชบัญญัติ  
คุ้มครองข้อมูลส่วนบุคคล  
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ  
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒  
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว  
มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า  
โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล



Understanding  
this new regulation



# โครงสร้าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ชื่อพระราชบัญญัติ

วันบังคับใช้

ขอบเขตการบังคับใช้

นิยาม

รัฐมนตรีผู้รักษาการ

**หมวด 1** คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**หมวด 2** การคุ้มครองข้อมูลส่วนบุคคล

**หมวด 3** สิทธิของเจ้าของข้อมูลส่วนบุคคล

**หมวด 4** สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**หมวด 5** การร้องเรียน

**หมวด 6** ความรับผิดทางแพ่ง

**หมวด 7** บทกำหนดโทษ

**บทเฉพาะกาล**

มาตรา 1

มาตรา 2

มาตรา 3 – มาตรา 5

มาตรา 6

มาตรา 7

มาตรา 8 – มาตรา 18

มาตรา 19 – มาตรา 29

มาตรา 30 – มาตรา 42

มาตรา 43 – มาตรา 70

มาตรา 71 – มาตรา 76

มาตรา 77 – มาตรา 78

มาตรา 79 – มาตรา 90

มาตรา 91 – มาตรา 96



# สาระสำคัญของ PDPA

## ขอบเขต การบังคับใช้



ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลฯ ที่เกิดขึ้นในราชอาณาจักร

ครอบคลุมถึงกรณีผู้ควบคุมและผู้ประมวลผลอยู่นอกราชอาณาจักร หากมีกิจกรรมดังนี้

- (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่
- (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร (GDPR Article 3 Territorial scope)

## ระยะเวลา บังคับใช้



พ้น 1 ปี นับแต่วันประกาศในราชกิจจานุเบกษา

ยกเว้นหมวดคณะกรรมการ และ  
สำนักงานมีผลทันที

## คำนิยาม



**ข้อมูลส่วนบุคคล** ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้  
ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรม  
โดยเฉพาะ

**ผู้ควบคุมข้อมูลส่วนบุคคล** (Data Controller) บุคคลหรือนิติบุคคลซึ่งมีอำนาจ  
หน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือ  
เปิดเผยข้อมูลส่วนบุคคล

**ผู้ประมวลผลข้อมูลส่วนบุคคล** (Data Processor) บุคคลหรือนิติบุคคลซึ่ง  
ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล  
ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล



## แจ้งให้ทราบ

ต้องแจ้งเจ้าของ  
ข้อมูลทราบถึง  
วัตถุประสงค์  
ของการเก็บ  
รวบรวม ใช้  
หรือเปิดเผย



## บทเฉพาะกาล

ให้ข้อมูลเดิมที่เก็บอยู่ก่อนวันที่  
กฎหมายใช้บังคับ ยังใช้หรือ  
เปิดเผยได้ตามวัตถุประสงค์  
เดิมที่ได้แจ้งไว้ต่อเจ้าของข้อมูล  
และต้องกำหนดวิธีการยกเลิก  
ความยินยอมให้สามารถแจ้ง  
ยกเลิกความยินยอมได้โดยง่าย

## การเก็บข้อมูล ม.22-23



ให้เก็บได้เท่าที่จำเป็นภายใต้  
วัตถุประสงค์อันชอบด้วย  
กฎหมายของผู้ควบคุมข้อมูล



## ความยินยอม

ต้องขอความยินยอม โดยต้องมีความชัดเจน ไม่เป็นการหลอกลวง  
หรือทำให้เจ้าของข้อมูลเข้าใจผิด

**การขอความยินยอม** ต้องทำเป็นหนังสือหรือทำโดยผ่านระบบ  
อิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอม  
ด้วยวิธีการดังกล่าวได้

การถอนความยินยอม เจ้าของข้อมูลถอนความยินยอม เมื่อใดก็ได้  
(เว้นแต่มีข้อจำกัด ตามที่กฎหมายกำหนด)

# สาระสำคัญของ PDPA



**ความยินยอม**  
ของผู้เยาว์  
คนไร้ความสามารถ  
และคนเสมือน  
ไร้ความสามารถ

- ผู้เยาว์**
  - ถ้าไม่ใช่ว่าอะไร ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพัง ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองด้วย
  - ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์
- คนไร้ความสามารถ**
  - ให้ขอความยินยอมจากผู้อุปการะที่มีอำนาจกระทำการแทนคนไร้ความสามารถ
- คนเสมือนไร้ความสามารถ**
  - ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ





# สาระสำคัญของ PDPA

## ข้อยกเว้น การบังคับใช้ ม.4



พระราชบัญญัตินี้ ไม่ใช้บังคับแก่

- (1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บ รวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัวของบุคคลหรือเพื่อกิจกรรมในครอบครัวของบุคคลเท่านั้น
- (2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงปลอดภัยของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหรือนิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
- (4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการ ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการพิจารณาตามหน้าที่และอำนาจ
- (5) การพิจารณาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
- (6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นทั้งหมดหรือแต่บางส่วน ในลักษณะใด กิจการใด หรือหน่วยงานใด ตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

ผู้ควบคุมข้อมูล ตาม (2) (3) (4) (5) และ (6) และที่ได้รับยกเว้นตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

# สาระสำคัญของ PDPA



**ข้อยกเว้น  
การจัดเก็บข้อมูล  
โดยไม่ต้องได้รับความ  
ยินยอม  
ม.24**

- (1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด
- (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- (3) เป็นการจำเป็นเพื่อ การปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- (4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนิน ภารกิจเพื่อประโยชน์สาธารณะ ของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอธิปไตยมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- (5) เป็นการจำเป็นเพื่อ ประโยชน์โดยชอบด้วยกฎหมาย ของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- (6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล



**ข้อยกเว้น  
การจัดเก็บข้อมูล  
จากแหล่งอื่น  
ม.25**

- ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่
- (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวัน นับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
  - (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

# สาระสำคัญของ PDPA



การเก็บข้อมูล  
Sensitive  
ม.26

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

- (1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
- (2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญาหรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้น ออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น
- (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
- (4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
  - เวชศาสตร์ป้องกัน หรืออาชีพเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง...
  - ประโยชน์สาธารณะด้านการสาธารณสุข
  - การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ...
  - การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น
  - ประโยชน์สาธารณะที่สำคัญ

กรณีประวัติอาชญากรรม ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย

# สาระสำคัญของ PDPA

## การใช้ หรือ การเปิดเผยข้อมูล ม.27



ห้ามมิให้ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปตามที่ให้ความยินยอม

การใช้หรือเปิดเผยในกรณียกเว้นตาม ม. 24 และ ม.26 จะต้องบันทึกการใช้และการเปิดเผยนั้น ด้วย



## การโอนข้อมูล ไปต่างประเทศ ม.28

ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ  
ทั้งนี้ต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด  
กำหนดย่อยกเว้น

- (1) เป็นการปฏิบัติตามกฎหมาย
- (2) ได้รับความยินยอมจากเจ้าของข้อมูล โดยได้แจ้งถึงมาตรฐานที่ไม่เพียงพอของปลายทางที่รับข้อมูลแล้ว
- (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อใช้ดำเนินการตามคำขอของเจ้าของข้อมูล ก่อนเข้าทำสัญญานั้น
- (4) เป็นการทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับบุคคลหรือนิติบุคคลอื่น เมื่อเจ้าของข้อมูลไม่สามารถให้ความยินยอมในขณะนั้นได้
- (5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- (6) เป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

(GDPR Article 45 Transfers on the basis of an adequacy decision safeguards)

กรณีมีปัญหาเกี่ยวกับมาตรฐานที่เพียงพอของปลายทาง ให้คณะกรรมการกำหนดเป็นผู้วินิจฉัย  
(GDPR Article 46 Transfer subject to appropriate)



## BCR ม.29

กำหนดหลักการ กฎเกณฑ์การให้  
ความคุ้มครองข้อมูลส่วนบุคคล  
ไปยังต่างประเทศและอยู่ในเครือ  
กิจการหรือเครือข่ายเดียวกัน  
เพื่อการประกอบกิจการหรือธุรกิจ  
ร่วมกัน หากมีนโยบายที่ได้รับ  
การตรวจสอบและรับรองจาก  
สำนักงาน สามารถโอนข้อมูลไปยัง  
ต่างประเทศได้ (เป็นไปตามที่  
คณะกรรมการกำหนด  
(GDPR Article 47 Binding  
corporate rules)



# สาระสำคัญของ PDPA



## สิทธิของเจ้าของข้อมูลส่วนบุคคล

มีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน

ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม



## สิทธิการ ระงับใช้ข้อมูล ม.34

(GDPR Article 18 (1) Right to restriction of processing)

- (1) ผู้ควบคุมอยู่ระหว่างการตรวจสอบความถูกต้อง
- (2) เมื่อเป็นข้อมูลที่ต้องลบหรือทำลายตาม ม.33(4) แต่เจ้าของขอให้ระงับแทน
- (3) เมื่อข้อมูลหมดความจำเป็นในการเก็บ แต่เจ้าของขอให้เก็บไว้เพื่อใช้ก่อตั้งสิทธิ การปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย
- (4) เมื่อผู้ควบคุมอยู่ระหว่างการพิสูจน์ตาม ม.32(1) หรือ (3)



## สิทธิโต้แย้งคัดค้าน ม.32

(GDPR Article 18 Right to restriction of processing)

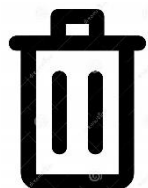
- (1) เป็นข้อมูลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตาม ม.24 (5) จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุม หรือ (6) ปฏิบัติตามกฎหมายของผู้ควบคุม และกำหนดให้ผู้ควบคุมต้องมีการพิสูจน์ได้ว่า
  - (ก) มีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
  - (ข) เป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามกฎหมาย
- (2) เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์ตลาดแบบตรง
- (3) เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์การศึกษาวิจัย ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม



## สิทธิในการ เคลื่อนย้ายข้อมูล ม.31

(GDPR Article 20  
Right to data  
portability)

- (1) ขอให้ผู้ควบคุมข้อมูลส่งหรือโอนข้อมูลไปยังผู้ควบคุมอื่น เมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
- (2) ขอรับข้อมูลจากผู้ควบคุมข้อมูลส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้



## สิทธิการ ลบข้อมูล ม.33

(GDPR Article 17 Right to be forgotten)

ขอให้ผู้ควบคุมข้อมูลลบหรือทำลาย หรือทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของได้ ในกรณีดังต่อไปนี้

- (1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์
- (2) เมื่อเจ้าของข้อมูลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผย และผู้ควบคุมไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผย ต่อไปได้
- (3) เมื่อเจ้าของข้อมูล คัดค้านการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล ตาม ม.32(1) และผู้ควบคุมไม่อาจปฏิเสธคำขอ
- (4) เมื่อข้อมูลถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

# สาระสำคัญของ PDPA

## หน้าที่ผู้ควบคุม ข้อมูลส่วนบุคคล ม.37



- (1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ทั้งนี้ต้องทบทวนมาตรการเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลง
- (2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุม ต้องป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- (3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่เกี่ยวข้องหรือเกิดความจำเป็นตามวัตถุประสงค์ หรือตามที่เจ้าของข้อมูลร้องขอ หรือ ถอนความยินยอม เว้นแต่เก็บรักษาเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น / การเก็บรักษาตาม ม.24 (1) ประวัติศาสตร์ จดหมายเหตุ วิจัยหรือสถิติ หรือ (4) ภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม หรือ ม.26 (5) (ก) เวชศาสตร์ การประเมินลูกจ้าง การวินิจฉัยทางการแพทย์ การรักษาทางการแพทย์ (เป็นการปฏิบัติตามกฎหมาย) หรือ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข การใช้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย หรือ เพื่อการปฏิบัติตามกฎหมาย  
ทั้งนี้ตามหลักการลบหรือทำลายข้อมูล หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวได้ ตามที่คณะกรรมการกำหนด
- (4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดจะไม่มีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล  
ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า
- (5) กรณีเป็นผู้ควบคุมข้อมูลที่อยู่ภายนอกราชอาณาจักร ต้องแต่งตั้งตัวแทนเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในราชอาณาจักร และต้องไม่มีข้อจำกัดในการรับผิดชอบใดๆ แทนผู้ควบคุมข้อมูล

กำหนดหลักเกณฑ์ข้อยกเว้นการแต่งตั้งตัวแทนของผู้ควบคุมตาม ม.37 (5) (ที่อยู่นอกราชอาณาจักร) ในกรณี

- (1) ผู้ควบคุมข้อมูลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด
- (2) ผู้ควบคุมข้อมูลไม่ประกอบอาชีพหรือไม่มีธุรกิจในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล Sensitive Data และไม่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

ให้ใช้หลักการนี้กับผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักร ที่มีผู้ประมวลผลนั้นโดยอัตโนมัติ

# สาระสำคัญของ PDPA

หน้าที่  
ผู้ประมวลผล  
ข้อมูลส่วนบุคคล  
ม.40



ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูล เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย  
จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย / แจ้งให้ผู้ควบคุมทราบถึงเหตุการณ์ละเมิดข้อมูลที่เกิดขึ้น / จัดทำและเก็บรักษา Log  
กรณีไม่ปฏิบัติตามหน้าที่ที่กำหนด ให้ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล



เจ้าหน้าที่  
คุ้มครองข้อมูล  
ส่วนบุคคล

กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (ม.41) ในกรณี

- (1) เป็นหน่วยงานของรัฐ ตามที่คณะกรรมการประกาศกำหนด
- (2) การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
- (3) กิจกรรมหลักของผู้ควบคุม หรือผู้ประมวลผล เป็นการเก็บรวบรวม ใช้ หรือเปิดเผย ตาม ม.26 Sensitive Data

(GDPR Article 37 Data protection officer)



หน้าที่ DPO ม.42

กำหนดหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- (1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล เกี่ยวกับการปฏิบัติตามกฎหมายนี้
- (2) **ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล** รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูล เพื่อให้เป็นไปตามกฎหมายนี้
- (3) ประสานงานและให้ความร่วมมือกับสำนักงาน
- (4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

# สาระสำคัญของ PDPA



## คณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล ม.8

- (1) ประธานกรรมการ : สรรหาและแต่งตั้งจากผู้มีความรู้
- (2) รองประธานกรรมการ : ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- (3) กรรมการโดยตำแหน่ง : 5 คน
  - ปลัดสำนักนายกรัฐมนตรี
  - เลขาธิการคณะกรรมการกฤษฎีกา
  - เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค
  - อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ
  - อัยการสูงสุด
- (4) กรรมการ ผู้ทรงคุณวุฒิ : 9 คน สรรหาและแต่งตั้งจากผู้มีความรู้
- (5) กรรมการและเลขานุการ : เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล



## สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล

กำหนดให้มีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองข้อมูลส่วนบุคคล

ส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

สำนักงานเป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการหรือรัฐวิสาหกิจ

คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- (1) ประธานกรรมการ สรรหาจากผู้ทรงคุณวุฒิ
- (2) กรรมการกำกับโดยตำแหน่ง ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- (3) กรรมการกำกับ : ผู้ทรงคุณวุฒิ : 6 คน
- (4) กรรมการและเลขาธิการ : เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม



# สาระสำคัญของ PDPA



## การร้องเรียน

เจ้าของข้อมูล มีสิทธิร้องเรียน  
ในกรณีผู้ควบคุม ผู้ประมวลผล  
รวมทั้งลูกจ้างหรือผู้รับจ้างของ  
ผู้ควบคุม ผู้ประมวลผล ฝ่าฝืน  
หรือไม่ปฏิบัติตามกฎหมาย



## คณะกรรมการ ผู้เชี่ยวชาญ

เพื่อพิจารณา  
เรื่องร้องเรียน  
ตรวจสอบ  
ข้อเท็จจริง  
ใกล้เคียง  
ข้อพิพาท และ  
ดำเนินการตาม  
อำนาจหน้าที่



## กรณีใกล้เคียง ไม่ได้

คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง

- (1) สั่งให้ผู้ควบคุม ผู้ประมวลผลปฏิบัติหรือแก้ไขการกระทำ  
ของตนให้ถูกต้องภายในระยะเวลาที่กำหนด
- (2) สั่งห้ามผู้ควบคุม ผู้ประมวลผลกระทำการที่ก่อให้เกิด  
ความเสียหายแก่เจ้าของข้อมูล หรือให้กระทำการใดเพื่อ  
บรรเทาความเสียหายนั้นภายในระยะเวลาที่กำหนด



## ความรับผิด ทางแพ่ง

ระบอบเขตของการละเมิดข้อมูล  
เน้นเป็นการฝ่าฝืนหรือไม่ปฏิบัติตาม  
บทบัญญัติ

- (1) กำหนดความรับผิดของ  
ผู้ควบคุมข้อมูลหรือ  
ผู้ประมวลผลข้อมูลเป็น  
ความรับผิดโดยเคร่งครัด  
(Strict Liability)
- (2) ให้อำนาจศาลสั่งให้ผู้ควบคุม  
ข้อมูลหรือผู้ประมวลผลข้อมูล  
ชดเชยค่าสินไหมทดแทนได้  
ไม่เกินสองเท่าของค่าสินไหม  
ทดแทนที่แท้จริง



## พนักงาน เจ้าหน้าที่ ม.37

พนักงานเจ้าหน้าที่ มีอำนาจ

- (1) มีหนังสือแจ้งให้ผู้ควบคุม ผู้ประมวลผล หรือผู้ใดมาให้ข้อมูล  
หรือส่งเอกสารหรือหลักฐานใดๆ เกี่ยวกับการดำเนินการหรือ  
การกระทำความผิดตามกฎหมายนี้
- (2) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อ  
คณะกรรมการผู้เชี่ยวชาญ  
ในกรณีตามข้อ (2) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของ  
เจ้าของข้อมูล หรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่  
ยื่นขอหมายศาล เพื่อเข้าไปในสถานที่ของผู้ควบคุม ผู้ประมวลผล  
หรือผู้ใด ในระหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตกหรือในเวลา  
ทำการของสถานที่นั้น



กำหนดอายุความฟ้องคดีเป็นการเฉพาะ เมื่อพ้นสามปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและ  
รู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิดหรือเมื่อพ้นสิบปีนับแต่วันที่มีการละเมิด  
ข้อมูลส่วนบุคคล

# สาระสำคัญของ PDPA



## บทลงโทษ โทษอาญา

สำหรับการกระทำที่เป็นความผิดร้ายแรง เช่น การแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น

		บทลงโทษ		
		ปรับ	จำคุก	ทั้งสอง
ม.79 ผู้ควบคุมข้อมูล ฝ่าฝืนหรือ ไม่ปฏิบัติตาม	ม.27 วรรคหนึ่ง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม)	<= 500,000	<=6 เดือน	✓ ยอมความได้
	ม.27 วรรคสอง (ได้รับข้อมูลตามวรรคหนึ่ง เปิดเผยนอกวัตถุประสงค์)			
	ม.28 (โอนข้อมูลไปต่างประเทศ) เกี่ยวกับข้อมูล ม.26 (Sensitive) โดยทำให้ผู้อื่นเกิดความเสียหาย	<=1,000,000	<=1 ปี	✓ ยอมความได้
	ม.27 วรรคสอง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกวัตถุประสงค์หรือ ส่งหรือโอนข้อมูลส่วนบุคคลที่ Sensitive ไปต่างประเทศ เพื่อแสวงหาผลประโยชน์ที่มิควรได้			
ม.80 ผู้ใด	ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตาม พ.ร.บ. นี้ ถ้านำไปเปิดเผยแก่ผู้อื่น	<=500,000	<=6 เดือน	✓
ม.81 นิติบุคคล	กระทำความผิดตาม พ.ร.บ. นี้ ถ้าการกระทำนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ผู้นั้นต้องรับโทษตามที่บัญญัติไว้ด้วย			

# สาระสำคัญของ PDPA



## บทลงโทษ โทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.82 ผู้ควบคุมข้อมูล ไม่ปฏิบัติตาม	ม.23 ไม่แจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์	<=1,000,000
	ม.30 วรรคสี่ ไม่ปฏิบัติตามเกณฑ์ในการให้เจ้าของเข้าถึงข้อมูล+รับสำเนา	
	ม.39 วรรคหนึ่ง บันทึกรายการให้เจ้าของข้อมูลและสำนักงานตรวจสอบ	
	ม.41 วรรคหนึ่ง จัดให้มี DPO หรือ ม.42 วรรคสอง สนับสนุน DPO หรือ วรรคสาม ไล่ DPO	
ม.83 ผู้ควบคุมข้อมูลฝ่าฝืน หรือไม่ปฏิบัติตาม	ม.21 เก็บ ใช้ รวบรวม เผยแพร่ต้องเป็นไปตามวัตถุประสงค์	<=3,000,000
	ม.22 เก็บ รวบรวม ให้เท่าที่จำเป็นตามที่กฎหมายกำหนด	
	ม.24 ข้อยกเว้นการเก็บจากเจ้าของข้อมูลโดยตรง	
	ม.25 วรรคหนึ่ง (ข้อยกเว้นการเก็บจากแหล่งอื่น)	
	ม.27 วรรคหนึ่งหรือวรรคสอง (ใช้เปิดเผยโดยไม่มีความยินยอม)	
	ม.28 โอนไปต่างประเทศ	
	ม.32 วรรคสอง (สิทธิคัดค้าน ใช้ เผยแพร่)	
	ม.37 หน้าที่ผู้ควบคุม	
	ขอความยินยอมโดยการหลอกลวง หรือใช้ผิดวัตถุประสงค์ (ม.21) ซึ่งได้นำมาใช้โดยอนุโลมตาม ม.25 วรรคสอง (แจ้งวัตถุประสงค์ใหม่)	
	ส่งหรือโอนข้อมูล ไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	

# สาระสำคัญของ PDPA



## บทลงโทษ โทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.84 ผู้ควบคุมข้อมูลฝ่าฝืน	ม.26 Sensitive วรรคหนึ่งหรือวรรคสอง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม)	<=5,000,000
	ม.27 วรรคหนึ่ง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือ วรรคสอง นอกเหนือวัตถุประสงค?	
	ม.28 ส่งหรือโอนข้อมูลไป ต.ป.ท. ซึ่งเป็นข้อมูล ม.26 Sensitive Data	
ม.85 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	ส่งหรือโอน ที่เป็นข้อมูล ม.26 Sensitive Data โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR))	<=1,000,000
	ม.41 วรรคหนึ่ง (DPO) หรือ ม.42 วรรคสองหรือวรรคสาม (การไล่ DPO)	
ม.86 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	ม.40 หน้าที่ผู้ประมวลผล โดยไม่มีเหตุอันควร	<=3,000,000
	ส่งหรือโอนข้อมูลโดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	
	ม.37(5) ผู้ควบคุมต้องตั้ง DPO ซึ่งได้นำมาใช้บังคับโดยอนุโลมตาม ม.38 วรรคสอง (การตั้งตัวแทนในราชอาณาจักร)	
ม.87 ผู้ประมวลผลข้อมูล	ส่งหรือโอนข้อมูลไป ตปท. ตาม ม.26 Sensitive Data วรรคหนึ่งหรือวรรคสาม (ประวัติอาชญากรรม) โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	<=5,000,000
ม.88 ตัวแทนผู้ควบคุมหรือตัวแทนผู้ประมวลผล	ไม่ปฏิบัติตาม ม.39 วรรคหนึ่ง (บันทึกรายการ) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.39 วรรคสอง (ตัวแทนผู้ควบคุม) และ ม.41 วรรคหนึ่ง (ตั้ง DPO) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.4 วรรคสี่ (การตั้งตัวแทนในราชอาณาจักร)	<=1,000,000
ม.89 ผู้ใด	ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ ตามมาตรา 75 หรือไม่ปฏิบัติตาม ม.76 วรรคหนึ่ง (แจ้งให้ส่งหนังสือ) หรือไม่อำนวยความสะดวกแก่ พนง.จนท. ตาม ม.76 วรรคสี่	<=500,000



# สาระสำคัญของ PDPA

## บทเฉพาะกาล



- ในวาระเริ่มแรก ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยกรรมการโดยตำแหน่ง ให้รองประธานทำหน้าที่ประธานเป็นการชั่วคราว  
ให้แต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิให้แล้วเสร็จภายใน 90 วันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ
- ให้ดำเนินการให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 90 วันนับแต่วันที่มีการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ให้ดำเนินการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายใน 1 ปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ
- ให้สำนักงานปลัดกระทรวง D.E. ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ให้รัฐมนตรี D.E. แต่งตั้งรองปลัดกระทรวง D.E. ทำหน้าที่เลขาธิการสำนักงานฯ เป็นการชั่วคราว และให้แต่งตั้งเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายใน 90 วัน นับแต่วันที่จัดตั้งสำนักงานฯ แล้วเสร็จ



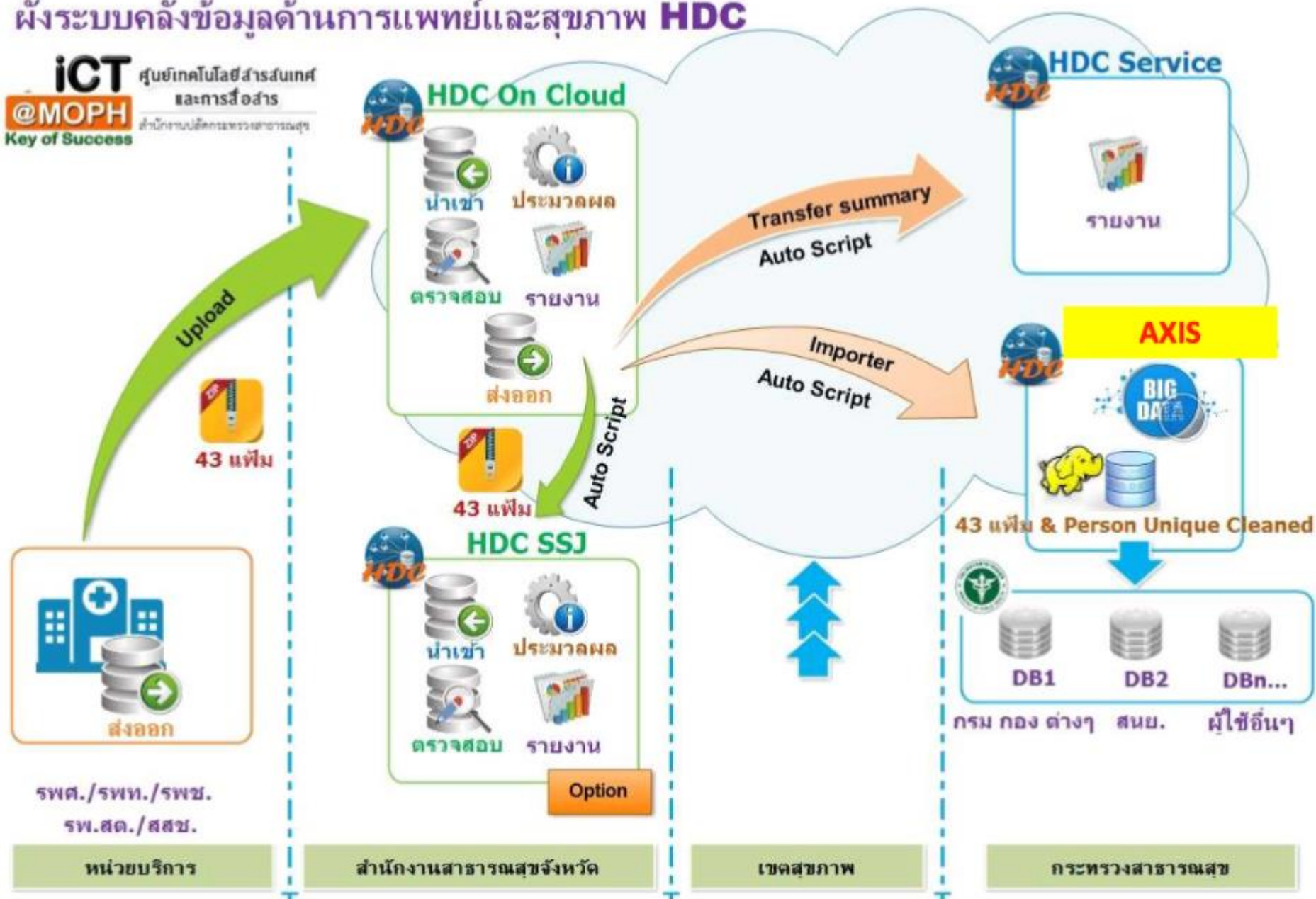
**การเชื่อมโยงแลกเปลี่ยนและการใช้ประโยชน์ข้อมูลผู้ป่วย**



# ผังระบบคลังข้อมูลด้านการแพทย์และสุขภาพ HDC

**ICT**  
**@MOPH**  
Key of Success

ศูนย์เทคโนโลยีสารสนเทศ  
และการสื่อสาร  
สำนักงานปลัดกระทรวงสาธารณสุข



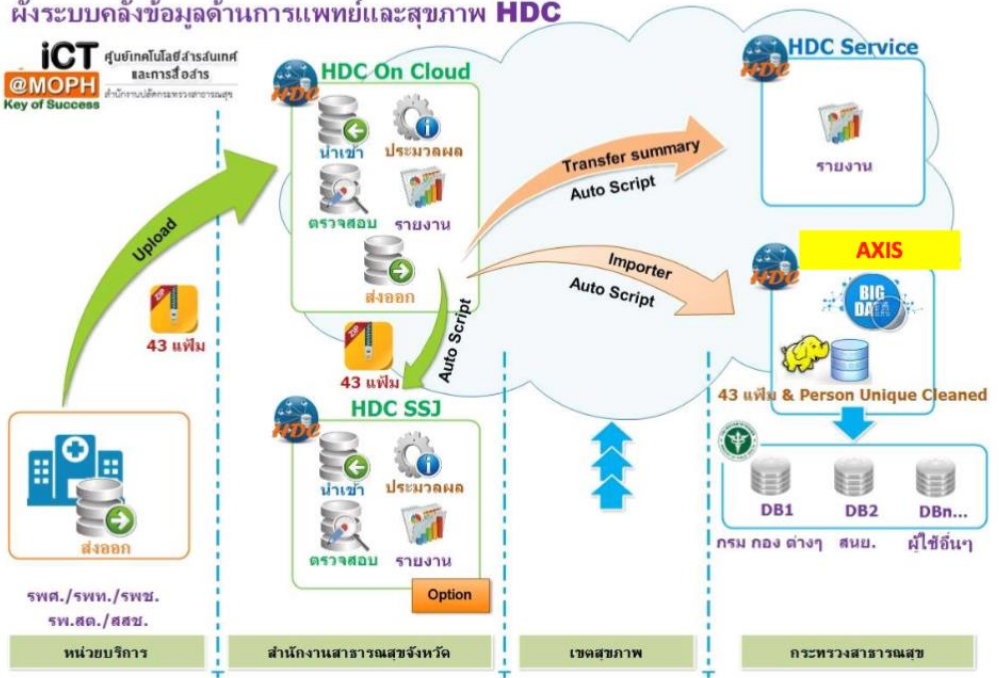




## ผังระบบคลังข้อมูลด้านการแพทย์และสุขภาพ HDC

ICT  
@MOPH  
Key of Success

ศูนย์เทคโนโลยีสารสนเทศ  
และการสื่อสาร  
สำนักงานปลัดกระทรวงสาธารณสุข



## ข้อมูล 43 แฟ้ม

- ข้อมูลเกี่ยวกับสุขภาพที่เป็นมาตรฐานเดียวกัน
- ได้รับจากผู้ป่วย/ผู้รับบริการ เก็บลงฐานข้อมูล
- ดึงออกจากฐานข้อมูลเป็น 43 แฟ้มตาราง
- ส่งต่อไปให้ผู้ที่เกี่ยวข้อง
- สสจ.รวบรวม ส่งผ่านระบบตามที่กำหนด / ตรวจสอบข้อมูล / ประมวลผลรายงานตามความต้องการของพื้นที่ / เผยแพร่ข้อมูลในจังหวัด
- สสจ.เชื่อมโยงข้อมูลด้วย HDC ไปยัง สป.สธ.

## ข้อมูล 43 แฟ้ม

ข้อมูลผู้ป่วยนอก / ผู้ป่วยใน ข้อมูลส่งเสริมป้องกัน

- Person ข้อมูลทั่วไปของ ปชช ในเขตรับผิดชอบ /ผู้มารับบริการ
- Address ข้อมูลที่อยู่ของผู้มารับบริการ นอกเขตหรือในเขต
- Death ข้อมูลประวัติการเสียชีวิตของ ปชช ในเขตรับผิดชอบ/รับบริการ
- Chronic ข้อมูลผู้ป่วยเรื้อรัง
- Card ประวัติที่มีหลักประกันสุขภาพ
- Home ข้อมูลครัวเรือนของ ปชช ในเขตรับผิดชอบ
- Village ข้อมูลทั่วไปและข้อมูลที่เกี่ยวข้องกับสุขภาพของชุมชน
- Disability ข้อมูลผู้พิการทุกคนที่อาศัยอยู่ในเขตรับผิดชอบ
- Provider ข้อมูลผู้ให้บริการของสถานพยาบาล
- Women ข้อมูลหญิงวัยเจริญพันธุ์
- Drugallergy ข้อมูลประวัติการแพ้ยาของผู้ป่วยที่มารับบริการ
- Functional ข้อมูลการตรวจประเมินความบกพร่องทางสุขภาพผู้พิการ..
- icf ข้อมูลการประเมินภาวะสุขภาพ ความสามารถ กลุ่มเป้าหมาย
- Service ข้อมูลการมารับบริการ และการให้บริการนอกสถานพยาบาล
- Diagnosis\_opd ข้อมูลการวินิจฉัยโรคของผู้ป่วยนอกและผู้มารับบริการ
- Drug\_opd ข้อมูลการจ่ายยาสำหรับผู้ป่วยนอกและผู้มารับบริการ
- Procedure\_opd ข้อมูลการให้บริการหัตถการและผ่าตัดของผู้ป่วยนอก
- Charge\_opd ข้อมูล คชจ. ของบริการแต่ละรายการ
- Surveillance ข้อมูลรายงานระบาดทางวิทยา
- Acceident ข้อมูลผู้มารับบริการที่แผนกฉุกเฉิน และแผนกทั่วไป
- Labfu ข้อมูลการตรวจทางห้องปฏิบัติการของผู้ป่วยเบาหวาน/ความดัน
- Chronicfu ข้อมูลการติดตามผู้ป่วยเรื้อรัง/ความดัน
- Admission ข้อมูลประวัติการรับผู้ป่วยไว้รักษาในโรงพยาบาล
- Diagnosi\_ipd ข้อมูลการวินิจฉัยโรคของผู้ป่วยใน
- Duig\_ipd ข้อมูลการจ่ายยาสำหรับผู้ป่วยใน
- ...



# Actions to take to prepare for the PDPA



เจ้าของข้อมูลส่วนบุคคล  
ผู้ป่วย / ผู้รับบริการ

## Data Subject Right

- Right to be informed
- Right to access
- Right to rectification
- Right to object
- Right to erasure
- Right to restrict processing
- Right to data portability



ข้อมูล 43 แพ้ม  
ข้อมูลผู้ป่วย/ผู้รับบริการ

## Data Protection Principle

- Consent & Choice*
- Purpose Specification
- Use Limitation
- Openness & Transparency and Notice
- Monitoring & Reporting
- Third Party & Vendor Management



โรงพยาบาล /  
สถานบริการ



สำนักงานสาธารณสุขจังหวัด  
/ สป.สาธารณสุข

## Obligation by Law

What Next to be Done


as the Controller / Processor / Vendor



## แนวทางการปฏิบัติตาม PDPA

# Key Changes of the PDPA

**Penalties**



≤ 5,000,000

The PDPA Penalties & fines apply to both Controllers and Processors

**Explicit consent**



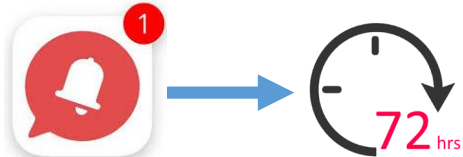
Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

**Limiting Collection, Use, Disclosure**



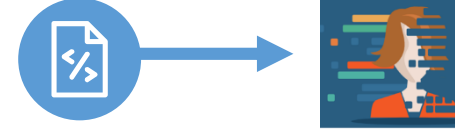
collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

**Breach notification within 72 hours**



Reported within 72 hours of first having become aware of the breach.

**Unified and expanded definition of personal data**



Unified interpretation of what constitutes personal data. New definition of data such as location and online identifier may result in additional compliance obligations (e.g. cookies now constitute an online identifier)

**Right to be forgotten**



data subject to have the data controller erase his / her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

**Right to access and portability**



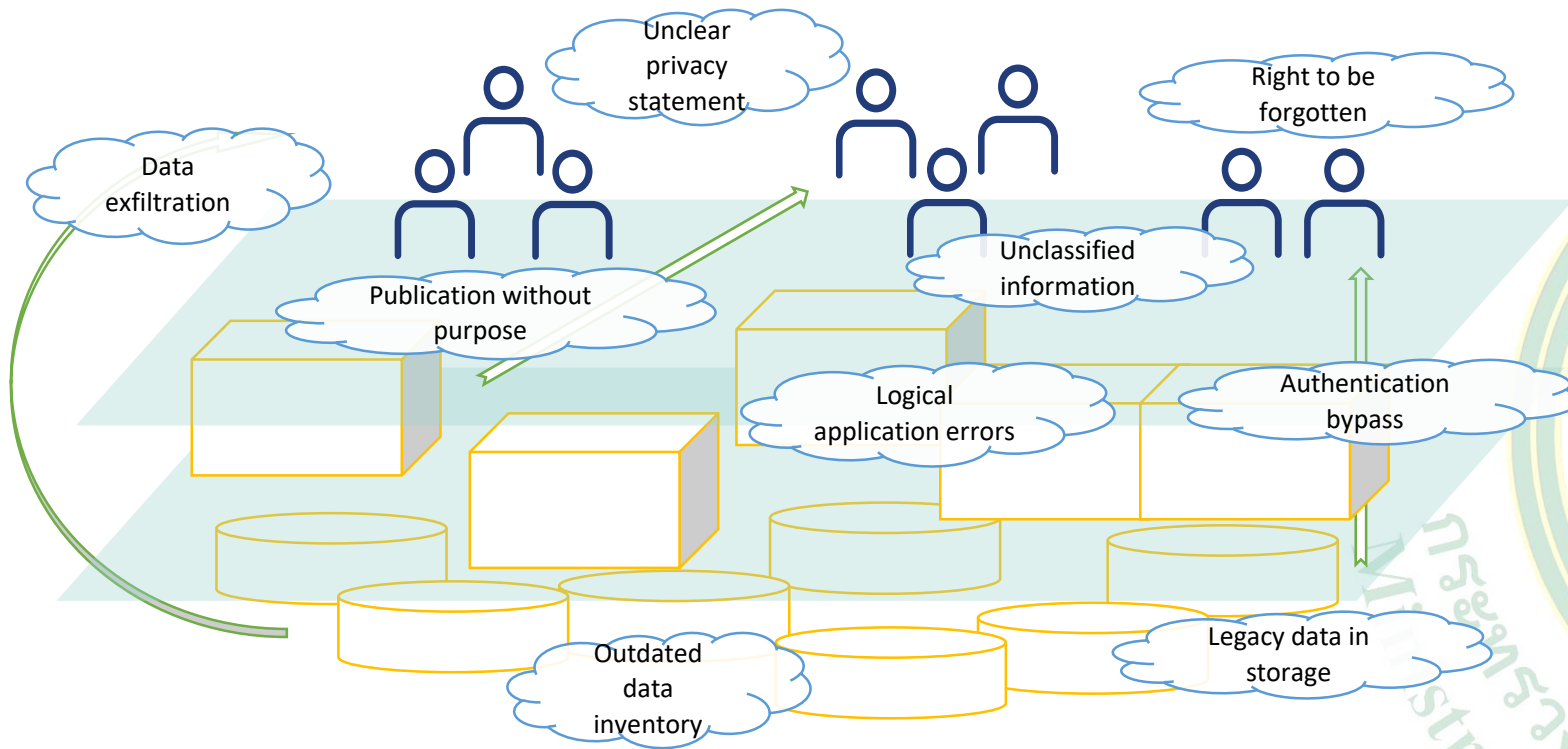
Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, in an electronic format (if practicable).


**Appointed Data Protection Officers**



Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for an organisation to demonstrate their compliance to the PDPA

# Key Challenge



 Data processor agreements

 Consent

 Cross-border data transfers

 Data subject rights

 Accountability

### Legal and Compliance



**PDPA introduces new requirements and challenges for legal and compliance functions.** If the PDPA is not complied with, organizations will face the heaviest fines. A renewed emphasis on organizational accountability will require proactive, robust privacy governance, requiring organizations to review how they write privacy policies, to make these easier to understand.

### Who Should Care

- CEO
- General Counsel
- Privacy Office
- Chief Risk Officer
- Chief Compliance officer



### Technology

PDPA changes to the ways in which **technologies are designed and managed. Documented privacy risk assessments** will be required to deploy major new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. **The concept of the Privacy Impact Assessment expected to become commonplace across organizations.** And organizations will be expected to look more into data masking, pseudo-anonymization and encryption.

- CIO
- Chief Information Security Officer



### Data

The information management will be challenged to provide clearer oversight on **data storage, transfer. The way you handle personal data has now changed**, how to comply with new data subject rights – rights to have data deleted and to have it ported to other organizations.

- Chief Data Officer
- Chief Operating Officer



# Organizational Perspectives

The PDPA impacts many areas of an organization



## Legal and Compliance



**A Revolution in Enforcement**



**Privacy Notices and Consent**  
Clarity and education is key



**Accountability**

Burden of proof now on the organization, not the individual



**Data Protection Officers**  
independent specialists



## Technology



**Data Protection Impact Assessments (DPIA)**



**Breach Reporting**

revise their incident management procedures and consider processes for regularly testing, assessing and evaluating their end to end incident management processes



**Encryption**

as means of providing immunity?



**Online Profiling**

Data subject have rights to opt out of and object to online profiling and tracking, significantly impacting direct-to-consumer businesses



## Data



**Data Inventories**

Identifying and tracking data  
what data they hold, where it is stored,  
and who it is shared with, by creating  
and maintaining an inventory of data  
processing activities



**New Definitions of Data**

New concept of pseudo-anonymous data  
concept of pseudo-anonymous data and at the same time  
expands the definition of personal data, placing a greater  
emphasis on data classification and governance.

# Organizational Perspectives

## Processes & Organization

Review business processes which handle personal data

- HP Processes (recruiting)
- Helpdesk processes
- Define the data controller / processor
- Direct marketing ?
- Invoicing
- Customer management
- ...

Controls : unified Risk Management

- Appoint DPO ?
- Embed control on Data privacy protection as a part of enterprise risk management alignment across regulations and compliance needs
- Org internal audit for PDPA related audits
- ...

## Legal & Compliance

## Cyber security & IT

Ensure adequate technology & IT Cyber measures

- Access controls to Personal Data
- Install breach detection and cyber incident management processes
- Install and Enforce secure software development processes
- Specific training & Awareness for IT staff on PDPA
- ...

Implement specific controls for personal data

- Encryption of data at rest
- Monitor data leaving the org
- Handling of test data
- Make staff aware of rules of the road
- ...

## Data Management

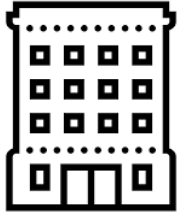
What Next to be Done

as the Controller / Processor / Vendor

# Actions to take to prepare for the PDPA

What Next to be Done

as the Controller / Processor / Vendor



## What organizations must do

- Develop policies and practices to ensure compliance
- Designation of key personnel to ensure compliance but organization remains ultimately responsible
- Staff education
- Develop a complaints response process – a process to take in requests for correction of DP and withdrawal of consent (depend on the legal )
- Transparency to the public regarding information of designated personnels and complaints response process
- Seek legal advice

### PDPA Readiness Assessment



1. Capture Business insight
2. Insight in current privacy situation
3. Develop Strategy and Roadmap

### PDPA Transformation Program



### Data Processing Inventory



Creating data inventory provides and overview of all data and insight in the risks attached to processing activities – Legal grounds, Data categories, Data subjects, Purposes, Security

### Third Party Procedures



External parties bring specific challenges for data controllers - Data Breach handling procedure, Vendor assessment, Data Processing agreements, Data subject right procedure



# Actions to take to prepare for the PDPA

What Next to be Done

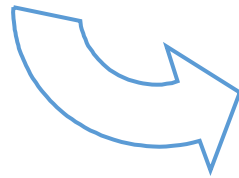
as the Controller / Processor / Vendor

## What organizations must do



ลักษณะหัวข้อร้องเรียนที่อาจเกิดขึ้น

- ความต้องการเข้าถึงข้อมูล จะต้องทำยื่นเรื่องขอหรือ Subject Access Request (SAR) แก่ผู้เก็บข้อมูล
- การขอแก้ไข/ลบข้อมูล
- Unfair processing
- Disclosure
- Employee privacy



การบริหารจัดการ เก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูล

- การจัดการ Record Processing
- การจัดการ Data Transfer
- การรับมือ Workload จากจำนวน การร้องเรียน / Call Center
- หลักการกำหนดคำถาม เพื่อประกอบการพิจารณา และทำ SAR
- ระบบการรายงานต่อ DPO
- การตอบ SAR เพื่อป้องกัน การร้องเรียนไปยังหน่วยงาน ตามกฎหมาย

การรับมือ Data Breach และการรายงาน

- ระบบการจัดการ Breach
- ทบทวนขั้นตอนการจัดการเหตุการณ์ และพิจารณากระบวนการสำหรับการ ทดสอบประเมินและประเมินจนจบ



- Review all Contract with your customer
- Review all Technical measure for Data Protection
- External Audit your SW and have assessment report



# Actions to take to prepare for the PDPA

“Specific issue to be considered in the development of a legal framework on data flow”

1

Distinction between transferring personal data within a jurisdiction or across abroad

2

Distinction between transfers to Controllers or Processors / Joint Controller

3

Contract / Lawfulness of Processing

4

Notification and Consent

5

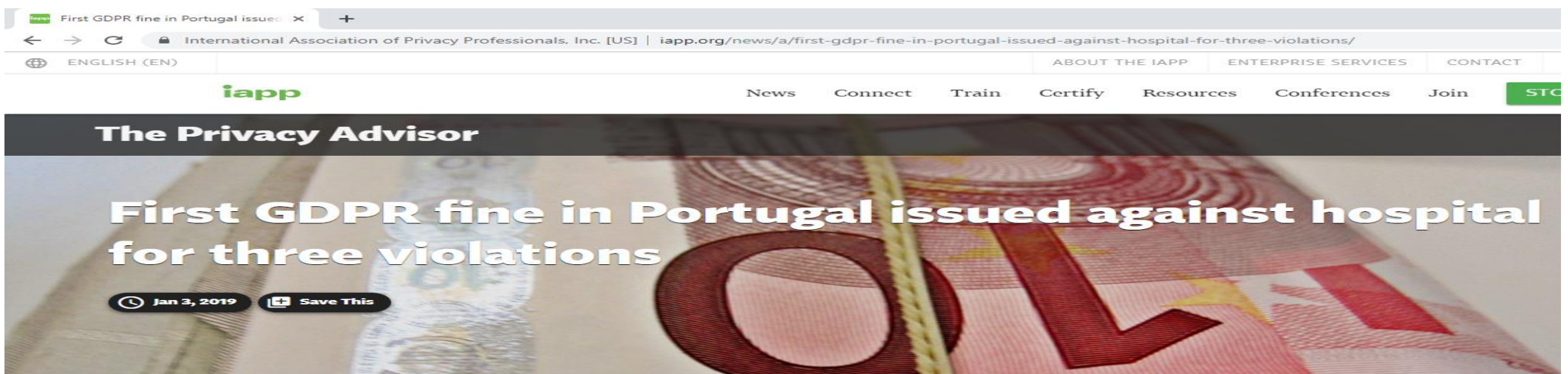
Achieve data processor / Code of Conduct and Standard

6

Record of Processing

7

Third Party Procedures



Centro Hospitalar Barreiro Montijo เป็น รพ. แรกใน EU ที่โดนปรับจาก GDPR ในเดือนมกราคม 2019

- เป็นโรงพยาบาลขนาด 500 เตียง
- โทษปรับมูลค่า 400,000 ยูโร หรือประมาณ 14 ล้านบาท
- DPA (Data Protection Authority) ของโปรตุเกส CNPD เป็นผู้สอบสวน
- โรงพยาบาล มีความผิดตาม GDPR 3 ข้อกล่าวหา

Centro Hospitalar Barreiro Montijo has been fined 400,000 euros for violating the General Data Protection Regulation.

The country's supervisory authority, Comissão Nacional de Protecção de Dados, found that there were three violations of the GDPR. First was a violation of Article 5(1)(c), a minimization principle, by allowing indiscriminate access to an excessive number of users, and a violation of Article 83(5)(a) a violation of the processing basic principles. For those, the fine was 150,000 euros.

The second, a violation of integrity and confidentiality as a result of non-application of technical and organizational measures to prevent unlawful access to personal data under Article 5(1)(f), and also of Article 83(5)(a), a violation of the processing basic principles. There, the fine was 150,000 euros.

Both of the above were punishable with a fine of up to 20 million euros or 4 percent of the total annual turnover.

# First GDPR fine in Portugal issued against hospital for three violations

Jan 3, 2019

Save This

ความผิดที่ 1 : ละเมิดหลักการ การดำเนินการเกี่ยวกับข้อมูลอย่างจำกัด (Minimization principle) และการอนุญาตให้เข้าถึงข้อมูลแบบ ไม่จำกัดสิทธิที่เหมาะสม เป็นการละเมิดมาตรา 5 (1)(c) และทำให้เกิดค่าปรับ ตามมาตรา 83 (5)(a) ซึ่งความผิดดังกล่าวนี้กำหนดค่าปรับในกรณีนี้ 150,000 ยูโรซึ่งความผิดนี้สามารถปรับได้สูงสุด 20 ล้านยูโร

## CHAPTER II

## Principles

## Article 5. Principles relating to processing of personal data

1. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

## CHAPTER VIII

## Remedies, liability and penalties

## Article 83. General conditions for imposing administrative fines

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;



# First GDPR fine in Portugal issued against hospital for three violations

Jan 3, 2019 Save This

ความผิดที่ 2 : ละเมิดหลักการ Integrity and Confidentiality เป็นการละเมิดมาตรา 5 (1)(f) ซึ่งเกิดจากไม่มีกลไก Technical & Organization Measure ต่อการประมวลผลข้อมูลส่วนบุคคล และทำให้เกิดค่าปรับ ตามมาตรา 83 (5)(a) ในการละเมิดข้อกำหนดหลักการปฏิบัติต่อข้อมูลส่วนบุคคล ซึ่งความผิดดังกล่าวนี้ กำหนดค่าปรับในกรณีนี้ 150,000 ยูโร

## CHAPTER II

### Principles

#### Article 5. Principles relating to processing of personal data

1. Personal data shall be:

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

## CHAPTER VIII

### Remedies, liability and penalties

#### Article 83. General conditions for imposing administrative fines

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;



# First GDPR fine in Portugal issued against hospital for three violations

Jan 3, 2019

Save This

ความผิดที่ 3 : ปรับโรงพยาบาลในฐานะ Controller มีหน้าที่ตามมาตรา 32 (1)(b) ในการกวดขัน การดำเนินการต่อการประมวลผล และการให้บริการที่กระทำต่อ ข้อมูลส่วนบุคคล โดยมีหลักการ Confidentiality, Integrity, Availability and Resilience อีกทั้งไม่ได้จัดให้มีการดำเนินการในด้าน Technical and Organization Measure ที่จะให้มีระดับการรักษาความปลอดภัยของข้อมูล สอดคล้องกับความเสี่ยง และขาดการทดสอบ ประเมินผล กลไกในด้าน Technical and Security Measure ดังกล่าว ซึ่งความผิดดังกล่าวนี้ กำหนดค่าปรับในกรณีนี้ 150,000 ยูโร ซึ่งความผิดนี้สามารถปรับได้ถึง 10 ล้านยูโร หรือ 2% ของรายรับ



## CHAPTER IV

### Controller and processor

#### Article 32. Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

สังคม Society

## First GDPR fine in Portugal issued against hospital for three violations

Jan 3, 2019 Save This

### สรุปข้อเท็จจริงจาก CNPD

- โรงพยาบาลได้กล่าวอ้างว่า ระบบงานนั้นเป็นระบบของ ก.สาธารณสุข มิใช่ของโรงพยาบาลเอง แต่ CNPD เห็นว่า ความรับผิดชอบของระบบโรงพยาบาล เป็นของโรงพยาบาลในฐานะ Controller
- ไม่มีเอกสารที่เทียบเคียง ถึงการกำหนดระดับความรู้ความสามารถของผู้ใช้งาน (ความเชี่ยวชาญทางการแพทย์) กับระดับที่กำหนดเป็น Profile ในการเข้าถึงข้อมูลคนไข้
- ไม่มีกฎระเบียบ และระบบการกำหนดการสร้าง และบริหารบัญชีผู้ใช้งานระบบของโรงพยาบาล
- เจ้าหน้าที่เทคนิค 9 คน สามารถเข้าถึงข้อมูลทางการแพทย์ที่ส่งวนไว้เฉพาะกลุ่มแพทย์
- ผู้ใช้งานในกลุ่มแพทย์นั้น ระบบมิได้แบ่งแยกความเชี่ยวชาญเฉพาะ หรือคลินิกที่ทำงานอยู่ ทำให้สามารถเข้าถึงข้อมูลได้ทั้งระบบ ซึ่งผิดหลักการ Need to Know & Minimization
- มีบัญชีผู้ใช้งานในระบบที่เป็น Profile กลุ่มแพทย์ 985 คน แต่บัญชีแพทย์ในโรงพยาบาลเพียง 296 คน
- ตั้งแต่เดือน พ.ย. 2016 มีการยกเลิกบัญชีแพทย์ในระบบเพียง 18 ราย ขาดการบริหารในเรื่องชื่อผู้ใช้งานระบบอย่างมีนัยสำคัญ
- เจ้าหน้าที่มีการปฏิบัติ แบบอิสระ มิได้มีสภาพบังคับ และตระหนักว่าสิ่งที่กระทำนั้น ละเมิดข้อกำหนดในกฎหมาย





**Q&A**

Contacts



T: 02 141 6991

F: 02 143 8036

Jakrapong.c[at]mdes.go.th

41/41