Digital
Law Landscape
For Government Agencies

Dr. Sak Segkhoonthod
Advisor (Digital Transformation)
ETDA

เอกสารประกอบการบรรยายเรื่อง "การเตรียมความพร้อมกฎหมายดิจิทัลใหม่ๆ กับงานสภากาชาดไทย สำหรับผู้บริหารและเจ้าหน้าที่" จัดโดย ศูนย์เทคโนโลยีสารสนเทศ

Digital Law Landscape

1 Cybersecurity
Law Landscape

PAYMENT

พ.ร.บ. ระบบการชำระเงิน

กำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบ
ระบบชำระเงินที่เป็นโครงสร้างพื้นฐานของประเทศ

ประกาศ ธปท. เรื่อง หลักเกณฑ์ทั่วไปในการกำกับดูแล การประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ

กำหนดมาตรการการรักษาความมั่นคงปลอดภัย
ทางระบบสารสนเทศ

INSURANCE

ประกาศ คปภ. เรื่อง หลักเกณฑ์ วิธีการออก และการเสนอขายกรมธรรม์และการชดใช้เงิน

กำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่
เกี่ยวข้องกับการออกกรมธรรม์ประกันภัย

SECURITY

ประกาศสำนักงาน ก.ล.ต. เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ

กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
หลักทรัพย์

TAX

ระเบียบกรมสรรพากร ว่าด้วยการจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์ และใบรับอิเล็กทรอนิกส์

กำหนดมาตรการรักษาความมั่นคงปลอดภัยของ
ระบบสารสนเทศที่เกี่ยวข้องกับการจัดทำใบกำกับภาษีอิเล็กทรอนิกส์หรือใบรับ
อิเล็กทรอนิกส์

GOVERNMENT

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

กำหนดธรรมาภิบาลข้อมูลภาครัฐที่ครอบคลุมมาตราการหรือระบบการรักษาความมั่นคง
ปลอดภัยในการเข้าสู่บริการดิจิทัลของหน่วยงานรัฐ

E-Transaction

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

ดูแลธุรกรรมออนไลน์ภาครัฐ เน้นสร้างความปลอดภัย
ความเชื่อมั่น & ระบบ

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศใน
การทำธุรกรรมออนไลน์ภาครัฐ

พ.ร.ฎ.วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พร้อม ประกาศ คธอ.

กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัย
ระบบสารสนเทศ ด้วยวิธีการแบบปลอดภัย
ของหน่วยงานของรัฐและเอกชน

กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์

ดูแลเพื่อให้การใช้งานออนไลน์ปลอดภัยสร้างความเชื่อมั่นทางเศรษฐกิจ

- **เพื่อป้องกัน และรับมือ Cyber Threat** พร้อมวิเคราะห์ แก้ไข/หยุดปัญหาให้เร็วที่สุด

  คณะกรรมการกำหนดรายละเอียด **ภัยคุกคาม ๓ ระดับ**

  - ไม่ร้ายแรง
  - ร้ายแรง
  - วิกฤต

  พร้อมแนวทางป้องกัน รับมือ
  ประเมิน ปราบปราม และระงับภัย

- **ปกป้อง CII ให้สามารถให้บริการได้อย่างต่อเนื่อง**

  เช่น ISP โทรคมนาคม สาธารณูปโภค (ไฟฟ้า ประปา) ทำงานผ่าน Regulator
  เพื่อไม่ให้ทับซ้อนกันและบูรณาการการทำงานระหว่างกัน

คณะกรรมการ
กำหนดกลุ่มภารกิจ
หรือบริการที่เป็น CII

(1) ด้านความมั่นคงของรัฐ
(2) ด้านบริการภาครัฐที่สำคัญ
(3) ด้านการเงินการธนาคาร
(4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
(5) ด้านการขนส่งและโลจิสติกส์
(6) ด้านพลังงานและสาธารณูปโภค
(7) ด้านสาธารณสุข
(8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

กำหนด**ลักษณะหน่วยงาน**ที่มีภารกิจหรือการให้บริการที่เป็น CII

*CII ย่อมาจาก Critical Information Infrastructure หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงสร้างการดูแล

- **คณะกรรมการระดับชาติ :**
  ดูแลภาพรวมเชิงนโยบาย
- **คณะกรรมการกำกับดูแล :**
  เพื่อให้การทำงานตามนโยบายมีประสิทธิภาพ
  ติดตามและรับมือภัยคุกคาม
  กำหนดแนวการทำงานและมาตรฐานขั้นต่ำ
- **คณะกรรมการบริหารสำนักงาน :**
  ดูแลงานบริหารทั่วไปของสำนักงาน
  ที่เป็นศูนย์กลางในการประสานงานและ
  เฝ้าระวังภัยคุกคาม
- **สำนักงาน NCSA**

	หน่วยงานของรัฐ	CII	หน่วยงานกำกับฯ	สำนักงานฯ
การรักษาความมั่นคงปลอดภัย	• **ปฏิบัติตามนโยบายและแผน** • **จัดทำประมวลฯ และกรอบมาตรฐาน:** โดยมีขั้นต่ำตามที่ กกม.กำหนด ประกอบด้วย การประเมินความเสี่ยง แผนการรับมือภัยคุกคาม • **แจ้งรายชื่อเจ้าหน้าที่ระดับบริหาร & ปฏิบัติการ**	• ปฏิบัติเช่นเดียวกับหน่วยงานของรัฐ • **ตั้ง CERT ของ CII หรือ CERT ของ Sector** • **แจ้งรายชื่อผู้ดูแลระบบ** • **ประเมินความเสี่ยง** • **Audit** อย่างน้อยปีละ 1 ครั้ง พร้อมรายงานสำนักงานฯ • **กำหนดแผนการเฝ้าระวังฯ** • **เข้าร่วมทดสอบความพร้อม**	• ปฏิบัติเช่นเดียวกับหน่วยงานของรัฐ • **ตรวจสอบมาตรฐานของ CII ในกำกับ** หากไม่แก้ไขแจ้ง กกม. เพื่อแจ้งผู้บริหารหน่วยงานสั่งการ	• **ให้ความช่วยเหลือ**
เกิดภัยคุกคาม	• **สนับสนุนข้อมูล บุคลากร เครื่องมือ แก่ กกม.**	• **ตรวจสอบ & ประเมินภัยคุกคาม** • **รายงานหน่วยงานกำกับ & สำนักงาน** (มีโทษ หากไม่รายงานโดยไม่มีเหตุสมควร) • **ปฏิบัติตามแผนการรับมือ** • **ปฏิบัติตามคำสั่ง กกม. & พนักงานเจ้าหน้าที่** (มีโทษ หากไม่ปฏิบัติตาม)	• **ให้ความช่วยเหลือ CII ในการรับมือ** • **แจ้งเตือน CII อื่นในกำกับ** • **แจ้งหน่วยงานกำกับ Sector อื่น**	• **ให้ความช่วยเหลือในการรับมือ** • **กกม. เป็นหลักในการรับมือภัยคุกคามระดับร้ายแรง** (หากเป็นระดับวิกฤติเป็นอำนาจ สมช.)

Cybersecurity

Implementation

แนวปฏิบัติสากล ที่อาจนำมาปรับใช้ในระหว่างรอหลักเกณฑ์

การใช้ **Cybersecurity Framework** (CSF)

ควบคู่กับมาตรฐานและคอนโทรลด้านความมั่นคงปลอดภัย

หมายเหตุ:

HIPAA = Health Insurance Portability and Accountability Act

FFIEC = Federal Financial Institutions Examination Council

NERC CIP = North American Electric Reliability Corporation Critical Infrastructure Protection

CSA = Cloud Security Alliance

มาตรฐานทั่วๆ ไป

- ISO/IEC 27001 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
- HIPAA กฎหมายคุ้มครองข้อมูลสุขภาพ (สหรัฐอเมริกา)
- FFIEC คู่มือการตรวจไอทีของหน่วยงานกำกับดูแลกลุ่มการเงิน (สหรัฐอเมริกา)
- NERC CIP มาตรฐานความมั่นคงปลอดภัยในกลุ่มผู้ผลิตไฟฟ้า (อเมริกาเหนือ)

มาตรฐานที่ Specific เฉพาะแต่ละ Sector

- บริการ Cloud computing - CSA Star
- กลุ่มสาธารณสุข - ISO 27799
- กลุ่มบริการชำระเงิน - PCI DSS (Data Security Standard)
- กลุ่มพลังงานไฟฟ้า NERC CIP

20 CRITICAL SECURITY CONTROLS

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercise

ที่มา: SANS

2

DATA

PRIVACY& PROTECTION

Law Landscape

PAYMENT

พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต

ปกป้องข้อมูลเครดิตที่ครอบคลุม
ข้อมูลส่วนบุคคล
(เป็นข้อยกเว้นของ PDPA)

ประกาศ ธปท. เรื่อง หลักเกณฑ์ทั่วไป ในการกำกับดูแลการประกอบธุรกิจ ระบบการชำระเงินภายใต้การกำกับ

กำหนดมาตรการดูแลการเก็บข้อมูลส่วนบุคคล

INSURANCE

ประกาศ คปภ. เรื่อง หลักเกณฑ์ วิธีการออก และการเสนอขายกรมธรรม์

กำหนดมาตรการดูแลข้อมูลส่วนบุคคล

TELCO

พ.ร.บ. กสทช.

กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคล
ของผู้ใช้บริการโทรคมนาคม

ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคม เกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม

กำหนดมาตรการดูแลข้อมูลส่วนบุคคล สิทธิเจ้าของข้อมูล
และหน้าที่ผู้ให้บริการ

รัฐธรรมนูญ 2560

ความเป็นส่วนตัวข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครอง ข้อมูลส่วนบุคคล
2562

GOVERNMENT

พ.ร.บ. ข้อมูลข่าวสารราชการ

กำหนดมาตรการดูแลข้อมูลส่วนบุคคลที่รัฐดูแล

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล

กำหนดธรรมาภิบาลข้อมูลภาครัฐ
ที่ครอบคลุมการดูแลข้อมูลส่วนบุคคล

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

ดูแลธุรกรรมออนไลน์ภาครัฐ เน้นสร้างความปลอดภัย
ลดความเสี่ยงต่อข้อมูลส่วนบุคคล & ระบบ

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ

แนวปฏิบัติดูแลข้อมูลส่วนบุคคลในการทำ
ธุรกรรมออนไลน์ภาครัฐ

HEALTHCARE

พ.ร.บ. สุขภาพแห่งชาติ

ปกป้องข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคล

ระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล

กำหนดเงื่อนไขการเปิดเผยข้อมูลสุขภาพ
พร้อมมาตการดูแล

ข้อมูลส่วนบุคคล คืออะไร ?

“ข้อมูลส่วนบุคคล” หมายความว่า

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถ
ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

แต่ไม่รวมถึงข้อมูลของ

ผู้ถึงแก่กรรมโดยเฉพาะ

: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

“personal data” means **any information relating to an identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

: General Data Protection Regulation (GDPR), EU

Examples of personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

: European Commission, *https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en*

ใคร

ที่มีสิทธิ & หน้าที่ ทำอะไร เก็บรวบรวม, ใช้, เปิดเผย

เจ้าของข้อมูลส่วนบุคคล (Data Subject)

- ให้**ความยินยอม** เท่าที่เหมาะสม
- รับทราบและใช้สิทธิที่มี

ผู้ควบคุมข้อมูลส่วนบุคคล (Controller)

- มีมาตรการดูแล Security ที่เหมาะสม และทบทวนสม่ำเสมอ
- ลบ ทำลายข้อมูล เมื่อพ้นระยะเวลาเก็บรักษา
- แจ้งเหตุละเมิด ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ
- ถ้าเป็น บจก. ตปท. ต้องแต่งตั้งตัวแทน และตั้ง **DPO**
- จัดทำ + เก็บรักษาบันทึกรายงาน

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor)

- เก็บ ใช้ เปิดเผยตามคำสั่ง
- จัดให้มีมาตรการดูแล Security ที่เหมาะสม
- แจ้งเหตุละเมิดให้ Controller ทราบ
- จัดทำ + เก็บรักษาบันทึกรายงาน

คณะกรรมการ

ที่ดูแล Law Compliance ตาม PDPA

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

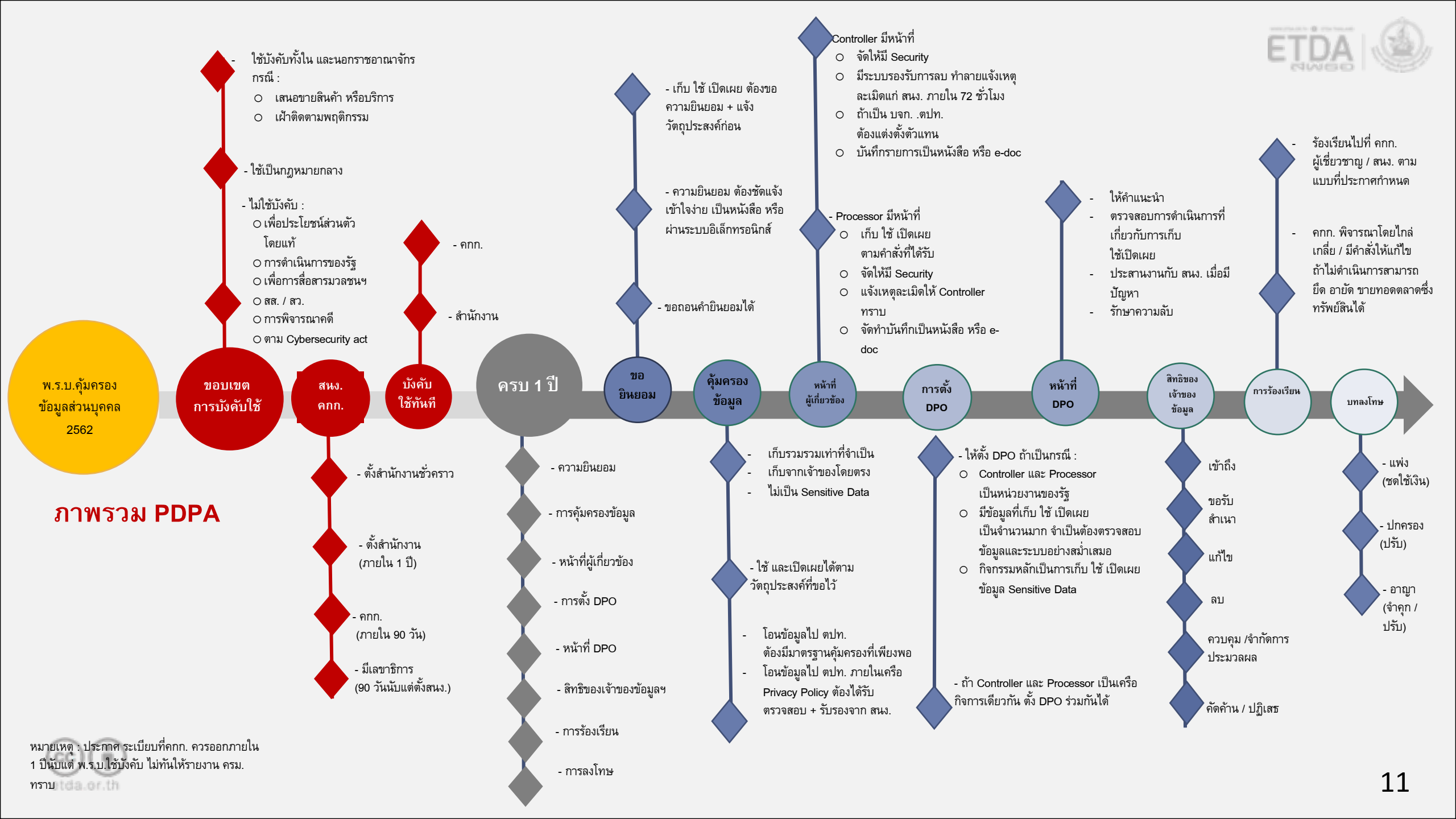
- จัดทำแผนแม่บท และแผนระดับชาติ
- กำหนดมาตรการและแนวทางการดำเนินงานเกี่ยวกับ DP
- ออกประกาศหลักเกณฑ์/มาตรการ
- วินิจฉัยชี้ขาด
- ส่งเสริมและสนับสนุนด้าน DP

คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียน
- ตรวจสอบการดำเนินการของผู้ที่เกี่ยวข้อง
- ไกล่เกลี่ยข้อพิพาท

Law Compliance ตามกฎหมายอื่น

ที่มีลักษณะเฉพาะ ลงลึก และ based on minimum requirement ของ PDPA พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล



หมายเหตุ : ประกาศ ระเบียบที่คกก. ควรออกภายใน 1 ปีนับแต่ พ.ร.บ.ใช้บังคับ ไม่ทันให้รายงาน ครม. ทราบ

3

ธรรมาภิบาลข้อมูลภาครัฐ

(Data Governance for Government)

(Data Governance for Government)

หลักการและสาระสำคัญ

ของพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

1 แผนระดับชาติ

- กำหนดให้มีการจัดทำแผนพัฒนารัฐบาลดิจิทัล
- แผนสอดคล้องกับยุทธศาสตร์ชาติและแผนระดับชาติ
- หน่วยงานของรัฐจัดทำหรือปรับปรุงแผนปฏิบัติการให้มีความสอดคล้อง

2 คณะกรรมการพัฒนารัฐบาลดิจิทัล

กำหนดให้มีคณะกรรมการพัฒนารัฐบาลดิจิทัล โดยมีนายกรัฐมนตรีเป็นประธาน มีอำนาจเสนอแนะนโยบายและจัดทำแผน วางกรอบธรรมาภิบาลข้อมูลภาครัฐ กำหนดมาตรฐาน ข้อกำหนดและหลักเกณฑ์

3 ธรรมาภิบาลข้อมูลภาครัฐ

กำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐ เป็นกรอบแนวทางการกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูล การมีระบบบริหารจัดการและคุ้มครองข้อมูล การมีมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูล และการกำหนดนโยบายและกฎเกณฑ์การเข้าถึงและใช้ประโยชน์ข้อมูลของหน่วยงานรัฐ

4 ปฏิรูปการทำงานและการให้บริการ (Digitalization)

- ให้หน่วยงานของรัฐจัดทำข้อมูลและบริการในรูปแบบดิจิทัลให้สอดคล้องกัน
- ให้หน่วยงานของรัฐจัดให้มีระบบการชำระเงินทางดิจิทัลและระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- มีมาตรการรักษาความมั่นคงปลอดภัยในการเข้าสู่บริการดิจิทัลของภาครัฐ

หลักการและสาระสำคัญ

ของพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

5 การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Integration)

- ให้หน่วยงานของรัฐเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันและลดการทำข้อมูลซ้ำซ้อน โดยใช้ข้อมูลที่หน่วยงานของรัฐอื่นจัดทำมาเป็นฐานข้อมูลก่อนจัดทำข้อมูลใหม่
- มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัล

6 บริการแบบเบ็ดเสร็จ ณ จุดเดียว

สนับสนุนและส่งเสริมให้หน่วยงานของรัฐเชื่อมโยงบริการดิจิทัลเพื่อให้บริการประชาชนในรูปแบบ One Stop Service

7 ศูนย์กลางข้อมูลเปิดภาครัฐ

ให้หน่วยงานของรัฐเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัล (Open Government Data) และให้มีศูนย์กลางข้อมูลเปิดภาครัฐ เพื่อให้ประชาชนสามารถเข้าถึงและร่วมตรวจสอบการทำงานภาครัฐ รวมถึงนำข้อมูลไปพัฒนาต่อยอดได้

8 กำหนดหน่วยงานของรัฐในการขับเคลื่อนรัฐบาลดิจิทัล

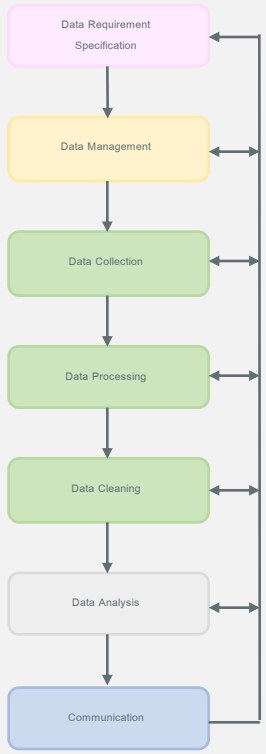
กำหนดให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เป็นหน่วยงานสนับสนุนการดำเนินงานของคณะกรรมการพัฒนารัฐบาลดิจิทัลและสนับสนุนการดำเนินการตามกฎหมายนี้

ทำไมองค์กรต้องทำธรรมาภิบาลข้อมูล

(Why Data Governance ?)

การไปสู่การเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data-driven Organization) → นโยบายข้อมูลองค์กร

ปฏิบัติตามกฎหมาย	สร้างความเชื่อมั่นในข้อมูลที่ออกจากองค์กรสู่สาธารณะ	เพิ่มประสิทธิภาพการทำงานภายใน	การใช้ข้อมูลทำงานร่วมกับผู้มีส่วนได้เสียเพื่อสร้างนวัตกรรม	ความโปร่งใสและการสร้างการมีส่วนร่วม
พรบ. คุ้มครองข้อมูลส่วนบุคคล	ข้อมูลที่เปิดตาม บทบาท หน้าที่ ความรับผิดชอบ	การไปสู่กระบวนงานที่ใช้ข้อมูลขับเคลื่อน	ข้อมูลเปิดสำหรับลูกค้า	สร้างการมีปฏิสัมพันธ์และการมีส่วนร่วม
พรบ. อื่น ๆที่องค์กรต้องส่งข้อมูลให้หน่วยงานกลางนั้น ๆ	ข้อมูลเปิดอื่น ๆที่มีคุณค่าสูง	กระบวนงานที่สามารถทำในแบบอัตโนมัติ	การแชร์ข้อมูลข้ามหน่วยงานที่เกี่ยวข้อง	การทำงานร่วมกันระหว่างทุกภาคส่วน
		การใช้ข้อมูลที่เกิดจากการวิเคราะห์เชิงลึกภายในองค์กร	การแลกเปลี่ยนข้อมูลสำหรับการทำธุรกรรมกับคู่ค้า	
			การใช้งานข้อมูลเชิงลึกของลูกค้าในการสร้างนวัตกรรมการให้บริการ	



Policy

คณะกรรมการธรรมาภิบาลข้อมูล

1 . กำหนดกลยุทธ์ เป้าหมาย

เจ้าของข้อมูล (ผู้รับผิดชอบข้อมูล)

ไม่เป็นข้อมูลส่วนบุคคล

2. กำหนดมาตรการ

เป็นข้อมูลส่วนบุคคล

Framework / Process

หัวหน้าบริกรข้อมูล

ผู้ควบคุมข้อมูลส่วนบุคคล

3. กำหนดนโยบาย ออกแบบ กระบวนการ

บริกรข้อมูล

ด้านควบคุม ข้อมูล

ด้านบริหาร จัดการข้อมูล

ด้านเทคนิค ข้อมูล

ด้านประสานงาน คุ้มครองข้อมูลส่วนบุคคล

คุณภาพ
- ความถูกต้อง
- ครบถ้วน
- ความต้องกัน
- ความพร้อมใช้

4. ปฏิบัติตามมาตรฐาน ข้อกำหนด หลักเกณฑ์ นโยบายและวิธีปฏิบัติ

Data Operation

ผู้ประมวลผลข้อมูล

ผู้ประมวลผลข้อมูล ส่วนบุคคล

Open Data

Shared Data

Exchange Data

Privacy Data

คุณภาพ
- ความเป็นปัจจุบัน
- ความพร้อมใช้

5. การนำข้อมูลไปใช้

Use

ผู้ใช้ข้อมูล

ผู้มีส่วนได้เสียกับข้อมูล ภายใน

ผู้มีส่วนได้เสียกับข้อมูล ภายนอก

เจ้าของข้อมูล ส่วนบุคคล

Audit

10. ตรวจสอบความคุ้มค่า ของการจัดทำธรรมาภิบาล ข้อมูลภาครัฐ

11. รายงานผลการตรวจสอบ

6. ตรวจสอบกฎหมาย นโยบาย คุณภาพ ความมั่นคงปลอดภัย

เจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคล

ผู้ตรวจสอบข้อมูล อิสระ

7. ตรวจสอบการปฏิบัติ คุณภาพ

8. ตรวจสอบคุณภาพ

9. รับฟังความคิดเห็น

คุณภาพ
- ตรงตามความต้องการของผู้ใช้

Version 1.0

Data Governance/Data Privacy Framework: Roles and responsibilities

	ผู้กำหนดนโยบาย (Policy Makers)		ผู้กำหนดมาตรการและแนวปฏิบัติ/บริการข้อมูล (Data Steward)				ผู้ประมวลผลข้อมูล (Data Processors)		ผู้ตรวจสอบข้อมูลอิสระ (Data Auditors)		ผู้มีส่วนได้เสีย (Stakeholders)			
	คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	เจ้าของข้อมูล (Data Owner)	ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Data Controller)	ด้านควบคุมข้อมูล (Data Controller)	ด้านบริหารจัดการข้อมูล (Data Manager)	ด้านเทคนิคข้อมูล (Data Custodian)	ผู้ประมวลผลข้อมูลส่วนบุคคล (Personal Data Processor)	ผู้ประมวลผลข้อมูล (Non-Personal Data Processor)	บริกรข้อมูลด้านตรวจสอบข้อมูล (Data Auditor)	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)	เจ้าของข้อมูลส่วนบุคคล (Data Subject)	ผู้ใช้ข้อมูล (Data Users)	ภายใน (Internal)	ภายนอก (External)
กลยุทธ์ เป้าหมาย (Strategies and Goals)	R A	C I	I S	I S	I S	I S	I S	I	C I	C I	C I	C I	I	I
นโยบาย (Data Policy)	A C	I S	R I	I S	C I	C I	I	I S	C I	C I	I	I	I	I
คุณภาพข้อมูล (Data Quality)	C I	R A	R I	R S	R I	R I	R I	C S	R C	R C	C I	C I	C I	C I
ความมั่นคงปลอดภัย (Data Security)	C I	R A	R A	R S	R I	R I	R I	C S	R C	R C	I	I	I	I
คุ้มครองข้อมูลส่วนบุคคล (Data Privacy)	A C	R A	R A	I S	R I	R I	R I	I	I	R A	A I	I	I	I
เชื่อมโยงแลกเปลี่ยนข้อมูล (Data Integration)	C I	R A	R A	R S	R A	R A	R A	C S	R C	R C	I	I	I	I
สื่อสารและอบรม (Communication and training)	C I	C S	R A	R S	I S	R S	I S	I S	C I	C I	I	I	I	I

หมายเหตุ : Responsible = ดำเนินการหลัก | Accountable = อนุมัติ | Support = ให้การสนับสนุน | Consulted = ให้คำปรึกษา | Informed = รับทราบข้อมูล

Version 1.1

WWW.ETDA.OR.TH : ETDA THAILAND

ETDA

สพธอ