สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

Office of the National Economic and Social Development Council

# โครงการแลกเปลี่ยนเรียนรู้ สศช. NESDC KM

# “PDPA ควรตระหนักแต่ไม่ (ควร) ตระหนก”

โดย นายสามารถ เจตนเสน

Senior Consultant และ Data Protection Officer



จัดโดย

กลุ่มพัฒนาระบบบริหาร (งานพัฒนาบุคลากร) สศช.

16 มิถุนายน 2565 เวลา 08.30 - 12.30 น.

ในรูปแบบออนไลน์ผ่านระบบ Zoom Meeting

# แนวทางการดำเนินการ

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

| มาตรา/บทลงโทษ | |
|---|---|
| | 1) กำหนดกลยุทธ์ กรอบแนวทางการกำกับดูแล โครงสร้างการกำกับดูแล กรอบการดำเนินงาน และผู้รับผิดชอบ ในการคุ้มครองข้อมูลส่วนบุคคล |
| (37-40) | 2) ศึกษาและวิเคราะห์สถานะหรือบทบาทขององค์กร ในฐานะ “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” |
| (24,26) | 3) ศึกษา และวิเคราะห์ เพื่อกำหนด “ข้อมูลส่วนบุคคล” (PII) และข้อมูลที่เป็น “Sensitive PII” ที่ต้องดำเนินการตามกฎหมายหรือกฎเกณฑ์ที่ประกาศบังคับใช้ |
| (39,82/1ล.) | 4) จัดทำ “Data Inventory” สำหรับกิจกรรมการรับ จัดเก็บ และใช้งานหรือประมวลผลข้อมูลส่วนบุคคล / ระบุฐานประมวล |
| (21,83/3ล.) (23,82/1ล.) | 5) จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy) และขั้นตอนปฏิบัติหรือคู่มือการปฏิบัติงาน ในการคุ้มครองข้อมูลส่วนบุคคล |
| (41,42,82/1ล.) | 6) แต่งตั้ง “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (DPO) และหมอบหมายหน้าที่ ตาม พ.ร.บ. ฯ |
| (37,83/3ล.) | 7) ประเมินผลกระทบและความเสี่ยงจากข้อมูลส่วนบุคคล Data protection Impact Assessment & Risk Assessment |

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

| มาตรา/บทลงโทษ | |
|---|---|
| | 8) จัดทำการกำหนดลำดับชั้นข้อมูล (Data Classification Policy/Procedure) |
| (30,82/1ล.) | 9) จัดทำเอกสาร และกระบวนการหรือระบบ เพื่อให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์ของใช้สิทธิ์ (Data Subject Rights Management) |
| (40/86/3ล.) | 10) จัดทำนโยบายหรือแนวปฏิบัติในการจัดจ้าง และแนวทางในการกำกับดูแล บุคคลหรือนิติบุคคลภายนอกที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Outsource) |
| (19/20/26) | 11) จัดทำกระบวนการจัดการการขอความยินยอม (Consent Management Procedure) |
| (37(3),83/3ล.) | 12) จัดทำนโยบายการจัดการ ระยะเวลาการเก็บข้อมูลส่วนบุคคล (Data Retention and Disposal Policy) |
| (28/79 (จ.6/0.5ล.)<br>(26/28 (จ.1 ปี/1ล.))<br>(26/28/83/3ล.) | 13) จัดทำนโยบายหรือแนวปฏิบัติในการ เปิดเผย ข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก หรือส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศ |

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

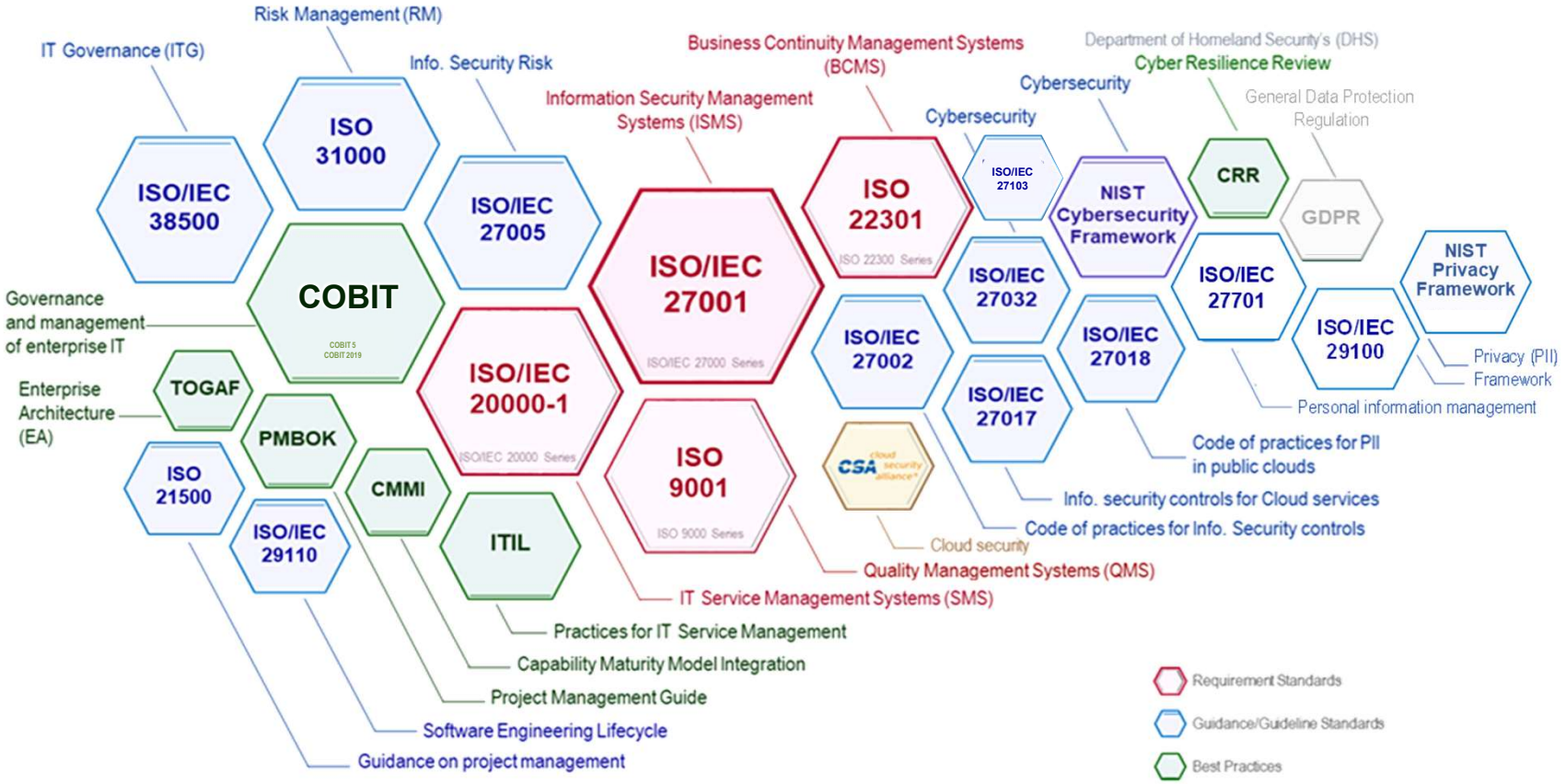
| มาตรา/บทลงโทษ | |
|---|---|
| (19/20/26) (40/86/3ล.) | 15) ทบทวนและแก้ไขหนังสือยินยอม (Consent) สัญญา (Contract) หรือข้อตกลง (Agreement) และขั้นตอนการขอความยินยอม ตามข้อกำหนดของ พ.ร.บ.ฯ |
| (23 25,82/1ล.) (21,83/3ล.) | 16) ประกาศความเป็นส่วนตัว Privacy Notice เพื่อให้เจ้าของข้อมูลส่วนบุคคล (Data subject) ได้รับทราบวิธีการประมวลผลข้อมูล |
| (37(4),83/3ล.) | 17) จัดทำเอกสาร และกระบวนการหรือระบบ เพื่อแจ้งเหตุการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน และ/หรือเจ้าของข้อมูลส่วนบุคคล |
| (37(1),83/3ล.) | 18) สร้างความตระหนัก และเสริมสร้างความรู้ให้กับผู้ปฏิบัติงานและผู้ที่เกี่ยวข้อง |
| (37(2),83/3ล.) (80/จ.6ด./0.5ล) (27/84/5ล.) | 19) กำหนดกรอบการประสานกับหน่วยงานกำกับดูแล หน่วยงานภาครัฐ และหน่วยงานความร่วมมืออื่น ๆ |

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

## แนวทางดำเนินการคุ้มครองข้อมูลส่วนบุคคล

- กฎเกณฑ์ GDPR (ดำเนินการตามกฎเกณฑ์และข้อกำหนดที่เกี่ยวข้อง)
- มาตรฐานสากล ISO/IEC 27701 Privacy Information Management (Aug. 2019)
  - ☐ ดำเนินการตามข้อกำหนดกรอบการบริหารจัดการและมาตรการคุ้มครองข้อมูลส่วนบุคคล
  - ☐ ดำเนินการตรวจรับรองตามข้อกำหนดระบบบริหารจัดการ Privacy Information Management
  - ☐ ขยายขอบเขตการตรวจรับรองมาตรฐาน ISO/IEC 27001 (Information Security Management System) ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคล และการจัดการในระบบคลาวด์
- มาตรฐานสากล ISO 29100 Privacy Framework (Implementation)
  - ☐ ดำเนินการตามข้อกำหนดกรอบการดำเนินงานในการคุ้มครองข้อมูลส่วนบุคคล
- มาตรฐาน NIST Privacy Framework *(16 Jan 2020)*
  - ☐ ดำเนินการตามข้อกำหนดกรอบการดำเนินงานในการคุ้มครองข้อมูลส่วนบุคคล
- แนวทางการเสริมสร้างความรู้ให้กับผู้ที่รับมอบหมาย “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer: DPO) และผู้ปฏิบัติงานที่เกี่ยวข้องตามกรอบ Privacy/Data Protection

# Standards & Best Practices



# Standards for Security and Privacy Management

- NIST Privacy framework (preliminary draft) :
  A Tool for Improving Privacy through Enterprise Risk Management

- ISO/IEC 29100 – Privacy framework
- ISO/IEC 29101 – Privacy architecture framework

- ISO/IEC 29134 – Guidelines for privacy impact assessment
- ISO/IEC 29151 / ITU-T X.1058 – Code of practice for PII protection
- ISO/IEC 29190 – Privacy capability assessment model
- ISO/IEC 29146 – A framework for access management
- ISO/IEC 27018 – Code of practice for protection of PII
  in public Clouds acting as PII processors

- General Data Protection Regulation (EU GDPR)

- ISO/IEC 27701 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines

- ISO/IEC 27001 - Information Security Management Systems — Requirements

- ISO/IEC 27002 - Code of practice for information security controls

- ISO/IEC TR 38505-1 – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data

- ISO/IEC TR 38505-2 – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management

- ISO/IEC 38500 – Governance of IT for the organization
- ISO/IEC TS 38501 – Governance of IT – Implementation guide
- ISO/IEC TR 38502 – Governance of IT – Framework and model
- ISO/IEC TR 38504 – Governance of IT – Guidance for principles – based standards in the governance of IT