เกริ่นนำและทำความรู้จัก

“Privacy” “Data Protection” และ GDPR :

ที่ปลุกกระแสความตื่นตัวของการทำธุรกิจดิจิทัล และวาระ Hot ในเวทีระดับโลก

สุรางคณา วายุภาพ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ทำไม Privacy จึงสำคัญ ?

สิทธิมนุษยชนขั้นพื้นฐาน

Universal Declaration of Human Rights
Article 12

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

GDPR
GENERAL DATA PROTECTION REGULATION

ความสัมพันธ์ระหว่าง
ความเป็นส่วนตัว และ ข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

ความเป็นส่วนตัว

เช่น สิทธิที่จะอยู่โดยลำพัง
(The right to be let alone)

ข้อมูลส่วนบุคคล

Data Subject (เจ้าของข้อมูล)

Data Controller (ผู้ควบคุมข้อมูล)

Data Processer (ผู้ประมวลผลข้อมูล)

คนไทย ให้ความสำคัญกับข้อมูลส่วนบุคคลมากขึ้น

ร้อยละของผู้ใช้อินเทอร์เน็ต เปรียบเทียบตามความคิดเห็นที่มีต่อกฎข้อบังคับหรือความคุ้มครองต่าง ๆ ในการซื้อสินค้า/บริการทางออนไลน์

แต่ความเป็นจริง ใช่อย่างนี้หรือไม่!!!

98.4	การปกป้องข้อมูลส่วนบุคคล
98.2	การป้องกันการรั่วไหลของข้อมูล (Data Breaches)
98.2	การป้องกันอาชญากรรมทางไซเบอร์ เช่น การฉ้อฉล อ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) การจารกรรม (Theft) การปลอมแปลงหรือละเมิดสิทธิส่วนบุคคล (Forgery and infringements of privacy)
97.8	การคุ้มครองผู้บริโภคทางออนไลน์
96.6	มีคำเตือนเรื่องอัตราภาษีอากรชัดเจน เมื่อซื้อสินค้าทางออนไลน์จากต่างประเทศ
96.5	กลไกการระงับข้อพิพาทของการซื้อสินค้า/บริการทั้งแบบออนไลน์ และออฟไลน์ข้ามพรมแดน (Online or Offline Cross-border Dispute Resolution)

เทคโนโลยีก้าวหน้า กับการดูแลข้อมูลส่วนบุคคล

Internet of Things (IoT)

เชื่อมต่อกับอินเทอร์เน็ต 8,400 ล้านชิ้น

ผู้ใช้อินเทอร์เน็ต 3,300 ล้าน

ทำให้มีข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมมีจำนวนมากขึ้น

สาเหตุ DATA Breach

ส่วนใหญ่มาจาก ภัยคุกคามไซเบอร์

หากข้อมูลรั่วไหลต้องทำอย่างไร ?

- รายงานเหตุการณ์
- รับมือ และบรรเทาความเสียหาย
- วิเคราะห์ และตรวจหาสาเหตุ
- ให้คำแนะนำเพื่อปรับปรุงระบบที่จัดเก็บข้อมูลส่วนบุคคล

Case Studies

AADHAAR — **รั่วไหล 1,000 ล้านคน**

EQUIFAX — **รั่วไหล 145 ล้านคน**

facebook — **รั่วไหล 87 ล้านคน**

UBER — **รั่วไหล 53 ล้านคน**

ข้อมูลของเราถูกนำไปใช้อะไรบ้าง?

Identity theft

“ถูกขโมยตัวตน”

เพื่อใช้ก่ออาชญกรรม และ
โจรกรรมข้อมูลทางการเงิน

Profiling

“ประมวลข้อมูลเพื่อใช้กำหนด Profile”

เพื่อเจาะโฆษณาหาประโยชน์
ทางการเมือง / การตลาด

Misuse

“ข้อมูลถูกขายให้บุคคลที่ 3”

เพื่อใช้ประโยชน์ทางการตลาด
เช่น กรณีของ Facebook และ
Cambridge Analytica

Tracking
Stalking
“ติดตาม สะกดรอย สอดแนม”

“SPAM”

เช่น เบอร์โทรศัพท์,
email เป็นต้น

ตัวอย่าง ภาคการบริการที่คาดว่าจะได้รับผลกระทบอย่าง อุตสาหกรรมการท่องเที่ยว

นักท่องเที่ยวชาวยุโรป

“เป็นนักท่องเที่ยวอันดับที่ 2”

ที่เดินทางมายังประเทศไทย

จำนวนนักท่องเที่ยว

6,511,195

คน

สร้างรายได้

480,776.31

ล้านบาท

แหล่งที่มา: จำนวนและรายได้ของนักท่องเที่ยว มกราคม ถึง ธันวาคม 2560P
กองเศรษฐกิจการท่องเที่ยวและกีฬา (ณ วันที่ 11 มกราคม 2561P)

ผลกระทบที่เกิดกับภาคธุรกิจ

“สูญเสียความน่าเชื่อถือ”

ทั้งนักลงทุนและกลุ่มลูกค้า

“ถูกดำเนินคดีทางกฎหมาย”

อาจต้องจ่ายค่าสินไหมทดแทน

“เกิดค่าเสียโอกาส”

อีกทั้งยังเป็นการเพิ่มต้นทุนค่าใช้จ่าย

“เสียเปรียบในการแข่งขันทางการค้า”

แบบสำรวจความตระหนักในการดูแลข้อมูลส่วนบุคคล

โดย สพธอ. (จำนวน 812 คำตอบ)

คนไทย

ผู้ใช้งานอินเทอร์เน็ต

กว่า 90%

เคยให้ข้อมูลส่วนบุคคลเพื่อเข้าถึงบริการออนไลน์ รองลงมาคือเพื่อชำระเงินและจัดส่งสินค้า

เพียง 9.5% อ่านข้อตกลงและนโยบาย

การใช้ข้อมูลของเว็บไซต์หรือ App ก่อนเข้าใช้งานโดยละเอียด

โดย **56%** ระบุว่าใช้เวลานานเกินไป

และ **50%** ระบุว่าข้อความเข้าใจยาก

16% ไม่เคยตั้งค่าความเป็นส่วนตัว (Privacy Setting) บน Social Network

45% ของคนกลุ่มนี้ ระบุว่า ไม่ทราบวิธีการตั้งค่า

กว่า 70% ตระหนักว่าเจ้าของข้อมูลมีบทบาทสำคัญที่สุดในการดูแลข้อมูล

61% มีความกังวลสูงสุด

หากมีการบันทึกข้อมูลส่วนบุคคลในการชำระเงินออนไลน์

แบบสำรวจความตระหนักในการดูแลข้อมูลส่วนบุคคล
โดย สพธอ. (จำนวน 812 คำตอบ)

ตัวอย่างพฤติกรรมบน Social Network ที่สุ่มเสี่ยงต่อ Privacy

65% เคยแชร์โลเคชัน

53% เคยอัปโหลดภาพหรือวิดีโอทันทีหลังถ่าย

15% เคยอัปโหลดภาพถ่ายตั๋วเครื่องบิน

DATA PRIVACY& PROTECTION

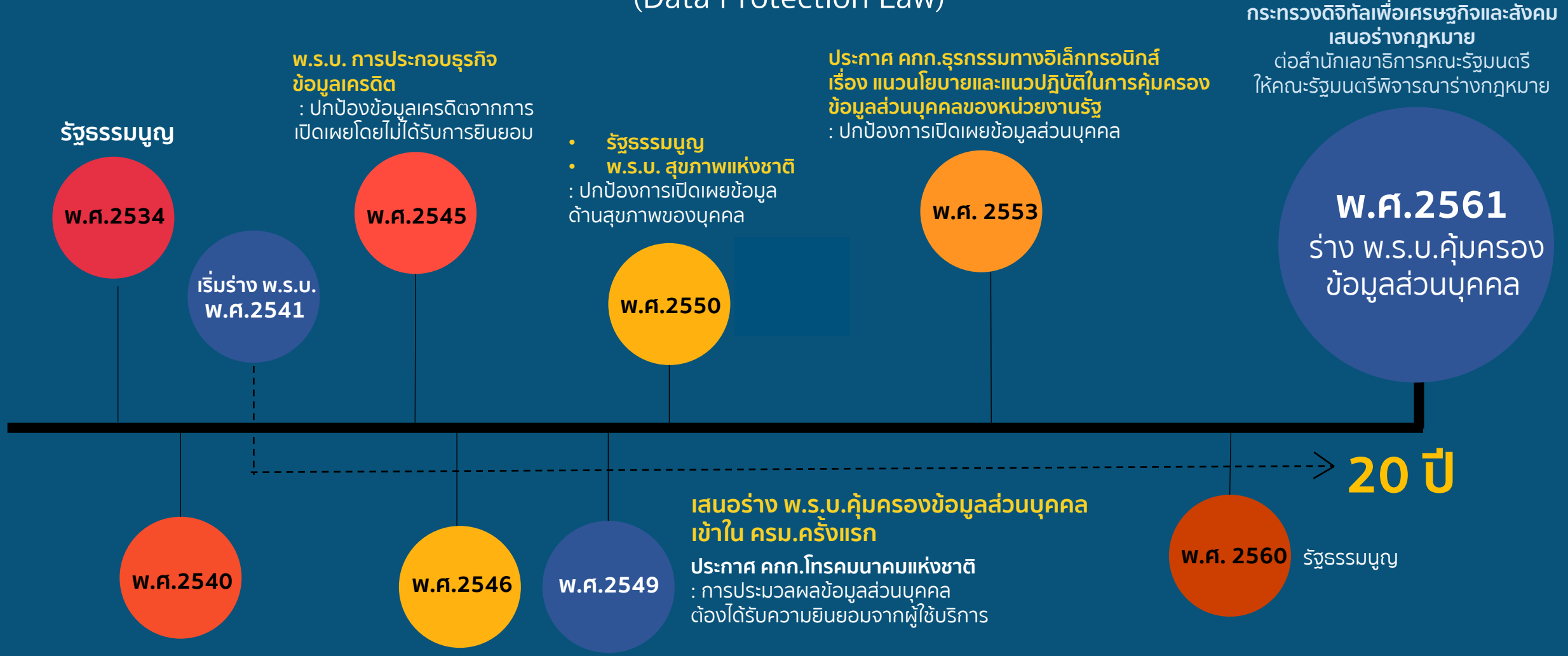
รัฐธรรมนูญ 2560

มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และ ครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

Timeline กฎหมายคุ้มครองข้อมูลส่วนบุคคลของคนไทย (Data Protection Law)



ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

จำแนกประเภทข้อมูล

หน้าที่ ผู้ควบคุมข้อมูล

กำหนดหน้าที่/ผู้รับผิดชอบ

สิทธิเจ้าของข้อมูล

ช่องทางติดต่อสื่อสาร

มาตรการความมั่นคงปลอดภัย

ดูแลระบบ IT

การละเมิดข้อมูลส่วนบุคคล

แจ้งเจ้าของข้อมูล/
หน่วยงานที่เกี่ยวข้อง

Soft Law & Self-Regulation

องค์กรร่วมกันจัดทำ

หลักการสำคัญของ GDPR

เพิ่มความเข้มงวดในการคุ้มครองข้อมูลส่วนบุคคล + เพิ่มเติมสิทธิของเจ้าของข้อมูล เช่น

- ข้อมูลส่วนบุคคลที่จัดเก็บต้องได้รับความยินยอมอย่างอิสระ ชัดแจ้ง
- แจ้งวัตุประสงค์การใช้ที่เข้าใจง่าย
- แจ้งแก้ไข/ลบ/ให้หยุดการประมวลผล เมื่อไม่จำเป็นต้องเก็บ/ไม่ประสงค์ให้นำข้อมูลไปใช้
- ขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น
- ผู้ควบคุมข้อมูลต้องจัดทำระบบให้เจ้าของข้อมูลต้องเข้าถึงข้อมูลของตนได้อย่างรวดเร็ว

เพิ่มมาตรการแจ้งเหตุกรณีมีการรั่วไหลของข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง พร้อมรายละเอียด แก่หน่วยงาน และเจ้าของข้อมูล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำกับดูแลบุคคลที่สาม เช่น Vendor ให้ปฏิบัติตามมาตรการดูแลข้อมูลส่วนบุคคล เช่น การกำหนดหน้าที่ตามสัญญาให้ชัดเจน

กำหนดบทลงโทษ หรือกำหนดค่าปรับตามความหนักเบาของการกระทำ โดยค่าปรับมี ๒ กรณี คือ

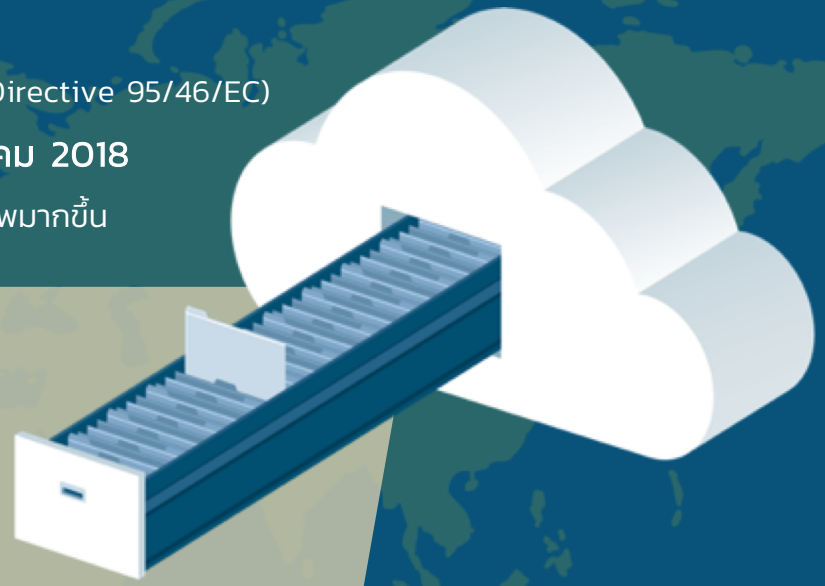
- breaches of controller or processor obligations ปรับสูงสุด 10 ล้านยูโร / 2% ของผลประกอบการทั่วโลกของปีที่แล้ว แล้วแต่จำนวนใดจะสูงกว่า
- breaches of data subjects' rights and freedoms ปรับสูงสุด 20 ล้านยูโร / 4% ของผลประกอบการทั่วโลกของปีที่แล้ว แล้วแต่จำนวนใดจะสูงกว่าแล้วแต่จำนวนใดจะสูงกว่า

กฎเกณฑ์การดูแลข้อมูลส่วนบุคคล ในระดับสากลที่เข้มข้นยิ่งขึ้น

หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล: EU

General Data Protection Regulation (GDPR: 2016)

- เป็นกฎหมายเกี่ยวกับ **PRIVACY & DATA PROTECTION** แทนที่ Data Protection Directive 1995 (Directive 95/46/EC)
- EU Commission รับรองวันที่ 27 พฤษภาคม 2016 **บังคับใช้**กับประเทศสมาชิก EU **วันที่ 25 พฤษภาคม 2018**
- หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ให้เจ้าของข้อมูลสามารถควบคุมข้อมูลของตนได้อย่างมีประสิทธิภาพมากขึ้น



ขอบเขตการใช้บังคับที่ไม่ได้จำกัดแค่ใน EU

ผลกระทบต่อประเทศไทย

1. หน่วยงานของรัฐและเอกชนไทย อาจได้รับกระทบ

หากมีการประมวลผลข้อมูลของคน EU ที่จะต้องปฏิบัติตาม GDPR

2. การโอนข้อมูลส่วนบุคคลมายังประเทศไทย

หากประเทศไทยไม่มีกฎหมาย หรือมีกฎหมายดูแลข้อมูลส่วนบุคคลที่ต่ำกว่า GDPR อาจส่งผลต่อการรับโอนข้อมูลส่วนบุคคลจาก EU มายังประเทศไทย เว้นแต่ผู้รับโอนมีกลไกการดูแล บังคับตามสิทธิของเจ้าของข้อมูล และการเยียวยาที่มีประสิทธิภาพเทียบเท่า GDPR

3. อาจถูกค่าปรับ เมื่อไม่ปฏิบัติตาม GDPR

การไม่ปฏิบัติตาม GDPR อาจถูกปรับ 4 เปอร์เซ็นต์ของผลประกอบการ หรือ 20 ล้านยูโร แต่ยังเป็นปัญหาว่าจะมีการบังคับในทางระหว่างประเทศอย่างไร

ประเภทของการละเมิด (Breach) ข้อมูลส่วนบุคคล

การละเมิดความพร้อมใช้ของข้อมูล (Availability Breach)

การทำลายข้อมูลส่วนบุคคลที่ไม่ไปเป็นตามกฎหมายหรือเกิดเหตุสุดวิสัย ทำให้ข้อมูลเสียหาย

การละเมิดความครบถ้วนสมบูรณ์ของข้อมูล (Integrity Breach)

การเปลี่ยนแปลงข้อมูลส่วนบุคคล

การละเมิดความลับของข้อมูล (Confidentiality Breach)

การเปิดเผยหรือเข้าถึงโดยไม่มีสิทธิของข้อมูลส่วนบุคคล

Four Steps to GDPR Planning

วัตถุประสงค์หลัก:
ตรวจจับและตอบสนองต่อภัยคุกคามก่อนเกิดการฝ่าฝืน แต่ถ้ามีการละเมิดเกิดขึ้นคุณจำเป็นต้องทราบรายละเอียดและผลกระทบที่แน่นอน

วัตถุประสงค์หลัก:
รู้ว่าข้อมูลอยู่ที่ไหนในองค์กร ใครสามารถเข้าถึงข้อมูลได้ และใครกำหนดมาตรการควบคุมการประมวลผลข้อมูล

วัตถุประสงค์หลัก:
จัดทำกระบวนการประเมินความเสี่ยงเพื่อสร้างความมั่นใจว่าการออกแบบและดำเนินการควบคุมถูกต้องเหมาะสม

วัตถุประสงค์หลัก:
สร้างโปรแกรมการปฏิบัติตามกฎระเบียบเพื่อให้การควบคุมมีประสิทธิภาพ

Source: RSAConference 2018

Phase	Assess	Design	Transform	Operate	Conform
Activity	• ประเมินความเสี่ยงและความพร้อมในการดูแลข้อมูลส่วนบุคคล • แผนเตรียมพร้อมตามGDPR • ระบุข้อที่อยู่ของข้อมูลส่วนบุคคล	• วางแผนการอบรม แผนการสื่อสารและมาตรฐานที่เกี่ยวข้อง • กำหนดมาตรฐานการจัดการข้อมูลและบริหารความมั่นคงปลอดภัยของข้อมูล	• พัฒนาขั้นตอนการปฏิบัติและเครื่องมือที่จำเป็น • จัดอบรม GDPR • พัฒนาระบบในลักษณะ Privacy by Design และ Security by Design	• นำไปปฏิบัติกับธุรกิจที่เกี่ยวข้อง • เฝ้าระวังด้านความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคลด้วยมาตรการทางเทคนิคและการจัดการ (TOMs) • จัดการความยินยอมและสิทธิในการเข้าถึงข้อมูล	• เฝ้าระวัง ประเมิน ตรวจสอบ รายงานความสอดคล้องกับ GDPR
Outcome	Assessments and roadmap	Defined implementation plan	Process enhancements completed	Operational framework in place	Ongoing monitoring and reporting
	ระบุผลกระทบจาก GDPR และวางแผนมาตรการทางเทคนิคและการจัดการ (Technical and Organizational Measures: TOMs)	มาตรการคุ้มครองข้อมูลส่วนบุคคล ที่ต้องปฏิบัติ	TOMs : การระบุข้อมูลส่วนบุคคล การจัดแบ่งประเภท และการจัดการและอภิบาลข้อมูล	เริ่มใช้ขั้นตอนการปฏิบัติใหม่ตาม GDPR	เฝ้าระวังการปฏิบัติตาม GDPR และรายงานผลการปฏิบัติให้ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกรับทราบ

Source: IBM's GDPR Readiness, Data Responsibility

สิ่งที่องค์กร ควรเตรียมความพร้อมก่อนกม.ข้อมูลส่วนบุคคลจะใช้บังคับ และเพื่อลดผลกระทบที่อาจเกิดจาก GDPR

ETDA สพธอ www.etda.or.th

- Data Protection by Design
- แต่งตั้ง Working Group ในองค์กร
- แต่งตั้ง DPO
- กำหนดประเภทของข้อมูล และมาตรการในการจัดการข้อมูล
- ทบทวน Data Protection Policy
- ควรทบทวนการบริหารจัดการ Personal Data และหลักเกณฑ์การให้ความยินยอม
- ทบทวนกระบวนการเข้าถึง แก้ไข ลบข้อมูล เมื่อได้รับการร้องขอ
- ทบทวน life-cycle ของการเก็บรักษาและทำลายข้อมูล

● เป็นกิจกรรมแรกๆที่ควรเริ่มดำเนินการก่อน

Source: IBM's GDPR Readiness, Data Responsibility

สิ่งที่องค์กร **ควรเตรียมความพร้อมก่อนกม.ข้อมูลส่วนบุคคล จะใช้บังคับ และเพื่อลดผลกระทบที่อาจเกิดจาก GDPR**

- จัดเตรียมข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
- ทบทวนมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่มีการโอนย้ายข้อมูลไป
- Document มาตราการรักษาความมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล
- จัดอบรมให้กับบุคลากร พนักงาน และเจ้าหน้าที่
- พัฒนาทักษะและกระบวนการตรวจสอบประเมิน (Audit)
- Privacy by Design และ Security by Design
- พัฒนากระบวนการแจ้งเตือน (Breach Notification)
- ได้รับงบประมาณและการสนับสนุนจากผู้บริหาร

● เป็นกิจกรรมแรกๆที่ควรเริ่มดำเนินการก่อน

Source: IBM's GDPR Readiness, Data Responsibility

พัฒนากระบวนการใน**การปกป้องข้อมูล**

Critical Data Protection Program

- ระบุและกำหนดข้อมูลส่วนบุคคล กำหนดมาตรการรักษาความมั่นคงปลอดภัย
- วิเคราะห์และจำแนกมิติที่สำคัญที่สุดของสภาพแวดล้อมข้อมูล
- ทำ GAP Analysis ของกระบวนการและมาตรการควบคุมความมั่นคงปลอดภัยข้อมูลสำคัญ
- ทำแผนการลดความเสี่ยง เพื่อจัดลำดับความสำคัญและทดสอบแนวทางแก้ไข
- ตรวจสอบกรอบการรักษาความมั่นคงปลอดภัย

Define

ข้อมูลส่วนบุคคลอะไร

- ทำความเข้าใจกลยุทธ์โดยรวมการรักษาความมั่นคงปลอดภัยข้อมูล
- กำหนดเป้าหมายการปกป้อง
- พัฒนาโครงสร้างโมเดลข้อมูล/อนุกรมวิธาน

Discover

ข้อมูลอะไร มีการใช้งานอย่างไร

- ทำความเข้าใจสภาพแวดล้อมข้อมูล โครงสร้าง และ lifecycle
- ดำเนินการตรวจค้น วิเคราะห์ และจำแนก อย่างต่อเนื่อง

Baseline

มีข้อกำหนดอะไรในการปกป้องข้อมูลสำคัญ

- ทำ baseline ความต้องการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ประเมินกระบวนการและมาตรการควบคุมความมั่นคงปลอดภัยข้อมูล
- ตรวจสอบ GAP และกำหนดแนวทางแก้ไข

Secure

จะวางแผน ออกแบบ และดำเนินการอย่างไร

- วางแผนและกำหนดลำดับความสำคัญของกระบวนการ Transformation ทางเทคนิคและกระบวนการทางธุรกิจ
- ออกแบบและดำเนินการเพื่อปกป้องข้อมูลสำคัญ ทำให้เข้าถึง และสอดคล้องกับเป้าหมายเติบโตทางธุรกิจ

Monitor

จะจัดการการปกป้องข้อมูลสำคัญอย่างไร

- พัฒนากรอบธรรมาภิบาล Risk metrics และกระบวนการเฝ้าระวัง
- ตรวจสอบกลยุทธ์และวิธีการในการปกป้องข้อมูลอย่างสม่ำเสมอ

5 กระบวนการของการรับมือและจัดการการละเมิดข้อมูลส่วนบุคคล

1 การรับมือ Incident และยกระดับการบริหารจัดการ (Escalation) ที่ทันต่อสถานการณ์ Single Channel of Escalation/ Documentation / Automated Detection & Alert

2 การประเมินความเสี่ยงอย่างต่อเนื่อง
Multi-Factor risk assessment / Legal Oversight / Documentation & Audit Trail

3 การรายงานและแจ้งเตือน เมื่อเกิดการละเมิดข้อมูลส่วนบุคคล
Approved Notification Template / Central Repository

4 การวิเคราะห์แนวโน้มและรายงานผลของการปฏิบัติควบคุมดูแลข้อมูล Establish Benchmarking / Track Key Indicators

5 การติดตามการเปลี่ยนแปลงของกฎเกณฑ์และข้อกำหนดต่าง ๆ
Monitor pending regulations / Implementing changes

WORKING TO A PLAN

คุณได้รับผลหรือไม่

องค์กรได้มีการประมวลผล การจัดเก็บ และการจัดการข้อมูลที่สามารถระบุตัวบุคคลได้ หรือข้อมูลส่วนบุคคล (หรือมีแผน) หรือไม่

YES

ข้อมูลที่สามารถระบุตัวบุคคลได้ดังกล่าวเป็นของคนที่มีถิ่นพำนักใน EU ซึ่งรวมถึงลูกค้าและ/หรือลูกจ้างใช่หรือไม่

YES

คุณได้เริ่มการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR แล้วหรือไม่

YES

คุณได้ประเมินความเสี่ยง หรือวิเคราะห์เกี่ยวกับ GDPR แล้วหรือไม่

ประเด็นที่คุณกังวลมากที่สุด

NO

หยุด
(แล้วแต่กรณี)

NO

ให้ความรู้ เกี่ยวกับ GDPR

กำหนดแผนของท่าน

การตอบสนองเมื่อเกิดเหตุการณ์ละเมิด (Breach Response)

คุณจัดการความเสี่ยงจากภัยคุกคามหรือการโจมตีทางไซเบอร์ขั้นสูงอย่างไร

กลยุทธ์ใดของท่านที่ใช้ในการระบุและตอบสนองเมื่อเกิด data breach

ขั้นตอนอัตโนมัติที่ใช้ในการลดระยะเวลาที่ breach exposure

Data Governance

คุณมีรายการการประมวลผลข้อมูลที่ถูกต้องหรือไม่

กลยุทธ์ใดของท่านที่ใช้ยืนยันว่าการเข้าถึงข้อมูลส่วนบุคคลมีความเหมาะสมและอยู่ภายใต้การควบคุม

คุณกำหนดนโยบายเกี่ยวกับ Data Governance อย่างไร

การประเมินความเสี่ยง (Risk Assessment)

ในกรณีปกติ องค์กรของท่านจัดการกับการประเมินความเสี่ยงอย่างไร

องค์กรของท่านมีกลยุทธ์ในการบริหารจัดการความเสี่ยงที่ครอบคลุมหรือไม่

การคุ้มครองข้อมูลส่วนบุคคลอยู่ภายในขอบเขตของกลยุทธ์ในการบริหารจัดการความเสี่ยงส่วนใด

การบริหารจัดการการปฏิบัติตามกฎระเบียบ (Compliance Management)

ในกรณีปกติ องค์กรของท่านจัดการกับการปฏิบัติตามกฎระเบียบอย่างไร

ท่านมีวิธีการระบุ จัดลำดับความสำคัญ และติดตามการปฏิบัติตามกฎระเบียบอย่างไร

ท่านมีวิธีจัดรายการข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้อง รวมทั้งข้อกำหนดตามกฎระเบียบอย่างไร

Source: RSAConference 2018

Facebook Cambridge / Analytica

ข้อมูลผู้ใช้งาน
เฟสบุ๊คหลุด

87

ล้านคน

ICANN / WHOIS

การเปิดเผยข้อมูล
ส่วนบุคคลกว่า

300

ล้านโดเมน

จะเข้าข่ายละเมิดข้อมูลส่วนบุคคลหรือไม่ ?

มีความเป็นไปได้ว่าจะมีการปิดการให้บริการหรือไม่ ?

YES

APPOINTED DPO: Have you appointed a data protection officer (DPO) who is responsible for processing activities?

NO

YES

DATA INVENTORY AND MAPPING: Do you know what data you collect and hold, where it is stored, how it is used, and how it is secured?

NO

YES

GAP ANALYSIS: Have you completed a fundamental assessment, comparing internal practices to the requirements of the GDPR?

NO

YES

PRIORITIZATION AND ACTION PLAN: Have you developed an action plan for achieving compliance based on your gap analysis? Are plans being implemented to address any major risks identified during your analysis?

NO

YES

SECURITY: Do you have and maintain a clear security policy, including industry standard practices such as hard drive encryption and data retention limitations?

NO

YES

DOCUMENTATION: Are you maintaining documentation of privacy and security efforts and issues?

NO

YES

LAWFUL BASIS FOR PROCESSING: Have you identified a lawful basis for processing personal data?

NO

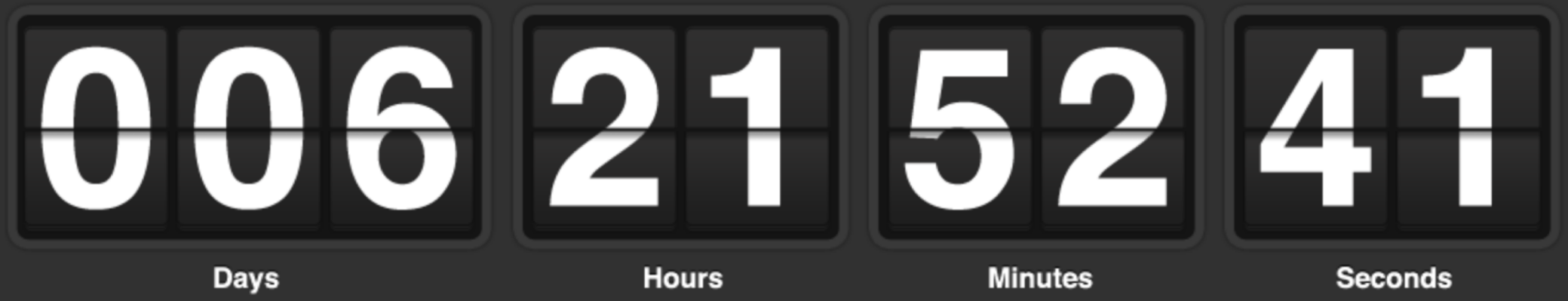
YES

PRIVACY NOTICE (TRANSPARENCY): Does your privacy notice clearly explain your privacy practices and explain the rights of your data subjects?

NO

Source: IAPP

EU GDPR COUNTDOWN



THANK YOU