ธรรมนิติ
DHARMNITI
www.dst.co.th

บทสรุป
PDPA

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

หลักการ แนวคิด ข้อกฎหมาย
กรณีศึกษาและแนวปฏิบัติ

พิมพ์ครั้งที่ 2 ปรับปรุงใหม่

บังคับใช้ 1 มิถุนายน 2565

กฤษฎ์ อุทัยรัตน์

บทสรุป
PDPA
กฎหมายคุ้มครองข้อมูลส่วนบุคคล

หลักการ แนวคิด ข้อกฎหมาย
กรณีศึกษาและแนวปฏิบัติ

บทสรุป PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล
หลักการ แนวคิด ข้อกฎหมาย กรณีศึกษาและแนวปฏิบัติ

โดย... กฤษฎ์ อุทัยรัตน์

พิมพ์ครั้งแรก : พฤศจิกายน 2563
พิมพ์ครั้งที่ 2 : สิงหาคม 2565

เจ้าของ	บริษัท ธรรมนิติ เพรส จำกัด
ที่ปรึกษา	ดารารัตต์ พืชมงคล
กองบรรณาธิการ	ศศิพินทุ์ อุษณีย์มาศ
ประสานงาน	ทิพสุคนธ์ วงษ์เมือง
พิสูจน์อักษร	ประนอม เพ็ชรสมัย, จันทร์จิรา ซื่อพร้อม
ออกแบบปก	วรรณา สนธิอนุเคราะห์
จัดรูปเล่ม	ปิติพัฒน์ อรุณวรวิวัฒน์

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

กฤษฎ์ อุทัยรัตน์.

บทสรุป PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล หลักการ แนวคิด ข้อกฎหมาย กรณีศึกษาและแนวปฏิบัติ.-- พิมพ์ครั้งที่ 2 กรุงเทพฯ : ธรรมนิติ เพรส, 2565. 508 หน้า.

1. การบริหารข้อมูลส่วนบุคคล. 2. การเปิดเผยข้อมูล--กฎหมายและระเบียบข้อบังคับ.

I. ชื่อเรื่อง.

342.0585

ISBN 978-616-302-235-6

จัดพิมพ์และจำหน่ายโดย บริษัท ธรรมนิติ เพรส จำกัด

178 อาคารธรรมนิติ ชั้น 4 ซอยเพิ่มทรัพย์ (ประชาชื่น 20) ถนนประชาชื่น
แขวงบางซื่อ เขตบางซื่อ กรุงเทพมหานคร 10800 โทรศัพท์ (02) 555-0713 โทรสาร (02) 555-0728

สนใจเสนอผลงานเขียนเพื่อตีพิมพ์กับธรรมนิติ ติดต่อ E-mail : book@dharmniti.co.th

คำนำ

(พิมพ์ครั้งที่ 2)

"บทสรุป PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล" หลักการ แนวคิด ข้อกฎหมาย กรณีศึกษาและแนวปฏิบัติ หรือ **PDPA LAW COMPENDIUM** : Principles and Concepts of Law and Practice เล่มนี้ ได้ตีพิมพ์ไปครั้งแรก เมื่อเดือนพฤศจิกายน 2563 และครั้งที่ 2 (ซึ่งเป็นการ Reprint จากการพิมพ์ครั้งแรก) ที่ผ่านมาอย่างต่อเนื่องและรวดเร็ว อาจารย์กฤษฎ์ อุทัยรัตน์ จึงขอถือโอกาสขอบคุณทุกท่านที่ได้ให้ความสนใจและไว้วางใจ จนทำให้หนังสือเล่มนี้ได้รับการตอบสนองที่ดีเยี่ยมจากบรรดาแฟนคลับ ลูกศิษย์ลูกหา ผู้ศึกษาในแวดวงคุ้มครองข้อมูลส่วนบุคคล การบริหารธุรกิจ บริหารทรัพยากรมนุษย์ และองค์การ รวมถึงผู้สนใจและผู้มีอุปการะคุณทุกท่านมา ณ ที่นี้ด้วยครับ

และเพื่อไม่ให้เป็นการสร้างความผิดหวัง ในครั้งที่ 3 นี้ ซึ่งถือได้ว่าเป็นการพิมพ์ครั้งที่ 2 ที่อาจารย์กฤษฎ์ อุทัยรัตน์ ได้ถือโอกาสปรับปรุง เปลี่ยนแปลง แก้ไข เพิ่มเติมข้อความ ถ้อยคำ รูปแบบต่างๆ โดยจัดให้มีรูปภาพประกอบแบบ Infographic (อินโฟกราฟิกส์) เพิ่มขึ้นและชัดเจนมากขึ้น ทั้งการขยายความเข้าใจและเชื่อมโยงข้อความในแต่ละบทแต่ละตอนให้อ้างอิงกลับไปกลับมาได้ง่ายขึ้น สะดวกต่อการค้นหาค้นคว้า ในส่วนของการประยุกต์ใช้ตัวอย่าง และกรณีศึกษา (Examples and Cases Study Application หรือ ECA) ก็ได้ แยกเป็นส่วนๆ แต่ละ ECA ให้ได้ทำความเข้าใจเป็นเรื่องๆ อีกทั้งเพิ่มเติมเนื้อหาให้ทันสมัยกับเหตุการณ์ในขณะพิมพ์ครั้งที่ 2 กับมีภาคผนวก

ให้ได้นำตัวบทกฎหมายของ พคข.2562/PDPA2019 มาสอดใส่เอาไว้ ให้สามารถเทียบมาตราทั้ง 96 มาตรา ได้ง่ายดาย ไม่ต้องแยกส่วนไปซื้อหาตัวบทกฎหมายมาเทียบเคียงให้เป็นที่วุ่นวายอีกด้วย

อย่างไรเสีย จากที่ได้กล่าวไว้ในคำนำของการพิมพ์ครั้งแรกว่าหนังสือเล่มนี้จะตอบโจทย์เบื้องต้นอันเป็นปฐมบทต่อยอดไปสู่ PDPA ใน Episode ต่อไป รวมถึงท่อนแยกของแต่ละ Episode ได้อีกด้วย แน่นอนครับว่าวันที่ 1 มิถุนายน 2565 เราๆ ท่านๆ ได้ใช้บังคับกันเต็มรูปแบบซะที และมันจะทำให้วิถีของ 3D ได้แก่ Data Subject, Data Controller และ Data Processer เปลี่ยนไปตลอดกาล เราไม่รู้ว่าสังคมของข้อมูลส่วนบุคคลในประเทศไทยจะเปลี่ยนไปในทิศทางใด แต่เปลี่ยนใหญ่อย่างแน่นอน หากคุณไม่พร้อมจะเปลี่ยน คุณจะเป็นผู้ถูกเปลี่ยนในที่สุด และไม่ว่าจะร้ายหรือดี การเตรียมความพร้อมเพื่อรับมือกับมัน เป็นเรื่องที่สมควรและมาเป็นอันดับต้นๆ ของวิถีแห่งคุณ วิถีที่ไม่ต่างไปจากวิถีแห่งเจได (Jedi) ใน Star Wars ที่คุณสามารถควบคุมการใช้พลัง (Force) ด้านสว่างหรือบวกได้ เพราะเราทุกคนต่างมีหน้าที่ใช้พลังด้านสว่างช่วยรักษาความสงบสุขของสังคม ถ้าเป็น PDPA ก็เน้นคุ้มครองข้อมูลส่วนบุคคลไม่ให้รั่วไหลหรือถูกละเมิด ซึ่งหนังสือเล่มนี้จะเป็นจุดเริ่มต้น พอจะช่วยให้เรียนรู้ฝึกฝนให้คุณเป็น "พาดาวัน (Padawan)" ในหนังพาดาวันจะต้องผูกเปียเล็กๆ และเรียกอาจารย์ของตัวเองว่า มาสเตอร์ (Jedi Master) เมื่อคุณถึงพร้อมที่จะรับมือกับกฎหมายเหนือกฎหมายตัวนี้ และถูกเลือกฝึกโดยอัศวินเจได (Jedi Knight) ด้วยการอบรม สัมมนา เรียนรู้ด้วยตนเอง หรือจากกูรูที่รู้จริงๆ ก็ได้ทั้งนั้น

ครับ กฎหมาย PDPA เป็นของใหม่ ง่ายเมื่อเริ่มต้นและต้องเปิดใจอยากเรียนรู้ แม้จะยากก็ต้อง**อยู่ให้เป็น** (เรียนรู้ที่จะปรับเปลี่ยนอย่างมีสติให้เท่าทัน) **เย็นให้ได้** (อดทนทำความเข้าใจ หาเคส ปรับใช้ให้เหมาะสมตามบริบท) **ใช้เวลาและรอคอย** (สร้างสมประสบการณ์ ให้ตกผลึก) อยากจะแนะนำให้ผู้อ่านได้เห็นว่า PDPA มันเรื่องใกล้ตัวเราเหลือเกินอยากให้ตระหนัก อยากให้ทำตัวให้เกิดพลังอยากเรียนรู้ ใฝ่รู้เอง ให้ได้มี Force Sensitive (สัมผัสได้ถึงพลังนั้น) แล้วเริ่มต้นเรียนรู้ ไม่ให้รู้ผิดๆ อย่าให้มีอวิชชา หรือให้ด้านมืดมาครอบงำจิตใจให้เข้าใจอะไรผิดเพี้ยน

เมื่อคุณเปิดกว้างในโลกแห่งการเรียนรู้ มันจะทำให้คุณมีรากฐานที่แข็งแรง แกร่ง และไม่อัตตา วิชา PDPA ก็ไม่ต่างกับการเอาเด็กใหม่ๆ ที่ไม่รู้อะไรเลยแต่มีความกระหายอยากจะรู้ มาฝึกโดยโยดา (แกรนด์มาสเตอร์ (Grand Master)) ณ วิหารเจได นั่นแหล่ะ สิ่งสำคัญอยากให้คุณเป็นเจไดในโลกของ PDPA ด้วยการละทิ้ง 3 ก (กลัว I โกรธ I เกลียด) เพราะจะเป็นการที่ทำให้ตัวคุณเองตกไปสู่ด้านมืด ฉะนั้นก็อย่ากลัวที่จะเรียนรู้และทำในสิ่งที่ถูกต้อง กล้าเปลี่ยนแปลง กล้าใช้เหตุผล อย่าโกรธกับภัยคุกคามทางไซเบอร์หรือการโจมตีข้อมูลส่วนบุคคลในทุกรูปแบบ อย่าโกรธคนที่คุณไม่เห็นด้วยอย่างมีอคติ อย่าโกรธที่คนนั้นคนนี้คิดต่างทำต่างจากเรา ให้มองว่ามันเป็นสีสันและช่วยเปิดโลกทัศน์ที่เราคาดไม่ถึงก็ได้ จากความต่างที่คิดเห็นไม่เหมือนกันนั้นทุกอย่างมันอาจเป็นไปได้ทั้งนั้น ในดีมีเสีย ในเสียมีดีว่ามั๊ย และอย่าเกลียดผู้คนและสังคมที่คุณอาศัยอยู่ไม่ว่าจะร้ายหรือดี ไม่ว่าจะกระทบและนำภัยมาสู่ข้อมูลส่วนบุคคลของคุณและตัวคุณก็ตาม

ขอพลัง (สติ) จงสถิตย์อยู่กับคุณ *(May the Force Be with You)* และจงสร้างไลท์เซเบอร์ (Lightsaber) อาวุธติดปัญญาในแบบที่เป็นของคุณด้วยตัวของคุณเอง แม้คุณจะใช้เวลาในการสร้างที่สมบูรณ์แบบนานแค่ไหน และกว่าจะได้มาให้คุณได้ใช้และอยู่กับมันแบบติดตามตัวคุณไปด้วยทุกแห่งหน และมันจะเป็นเกราะคุ้มครองความอ่อนไหวอ่อนแอของจิตที่คร้านต่อการเรียนรู้อย่างต่อเนื่องได้เป็นอย่างดี จงสร้างองค์ความรู้ด้าน PDPA ให้ทันและให้ไว แม้ว่ามันจะเป็นเรื่องใหม่แต่มาเร็วและแรง อันนี้ ลุค สกายวอล์คเกอร์ (Luke Skywalker) กล่าวไว้และอาจารย์เองเอามาผสมผสานให้กลมๆ กลืนๆ อีกหน่อย

คิดว่าดีและหวังว่าหนังสือเล่มนี้จะช่วยสร้างไลท์เซเบอร์ให้เป็นอาวุธติดปัญญาให้กับคุณผู้อ่านได้ ไม่มากก็น้อย ขอบคุณสำหรับทุกคนไว้ ณ ที่นี้อีกครั้งและทุกๆ ครั้งนะครับ ขอบคุณจริงๆ

ด้วยจิตคารวะ
ขอพลัง (สติ) จงสถิตย์อยู่กับคุณ
อาจารย์กฤษฎ์ อุทัยรัตน์

ปรับปรุง 1 สิงหาคม 2565

สารบัญกุญแจสำคัญ*
(Keyword Index)

** ใช้สืบค้นประเด็น หัวเรื่อง สาระสำคัญที่ผู้เขียนมองและเล็งเห็นว่าเป็น Keyword ที่น่าสนใจ เน้นย้ำเป็นพิเศษ ควบคู่กับสารบัญทั่วไปแบบผสมผสาน*

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ (Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

สารบัญกุญแจสำคัญ
(Keyword Index)

บทที่ 1

ทำไมต้องให้ความสำคัญ กับข้อมูลส่วนบุคคล

ทำไมต้องให้ความสำคัญกับข้อมูลส่วนบุคคล

เป็นคำถามที่ตอบได้หลากหลาย "ข้อมูลส่วนบุคคล" Personal Data : PD[1] หรือ PII[2] (Personally Identifiable Information) เป็นยิ่งกว่าทองคำในยุคที่ใคร ๆ หรือธุรกิจต้องการข้อมูลจากลูกค้า ลูกจ้าง คู่ค้า ผู้มีส่วนได้เสียกับธุรกิจหรือกิจกรรมซึ่งต้องพึ่งพาข้อมูลส่วนบุคคล ไม่ว่าจะเป็นชื่อนามสกุล อีเมล เบอร์โทรศัพท์ ที่อยู่อาศัย ข้อมูลความเป็นส่วนตัวทั้งหลายเหล่านี้ล้วนแล้วแต่เป็นข้อมูลส่วนบุคคลทั้งสิ้น จึงต้องการความคุ้มครองปกป้องข้อมูลของเจ้าของข้อมูล (Data Subject) ซึ่งหมายถึง บุคคลผู้ซึ่งข้อมูลส่วนบุคคลนั้นระบุไปถึงได้นั่นเอง ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของ (Ownership) ข้อมูลหรือเป็นคนสร้างหรือเก็บรวบรวมข้อมูลนั้นๆ เท่านั้นนะครับ และคำว่า "บุคคล" (Natural Person) ก็ย่อมหมายถึงบุคคลธรรมดาที่ยังมีชีวิตอยู่ ไม่ได้เหมารวมถึงนิติบุคคล (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น ห้างหุ้นส่วนสามัญ ห้างหุ้นส่วนจำกัด บริษัทจำกัด บริษัทมหาชนจำกัด สมาคม มูลนิธิ สหภาพแรงงาน หรือองค์การอื่นใดนะครับ

---

[1] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA 2019 มาตรา 6 "ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ สอดคล้องกันไปกับ GDPR (General Data Protection Regulation Act: EU, Article 4 (1)) แปลเป็นไทย หมายความว่าข้อมูลสารสนเทศใด ๆ ก็ตามที่เกี่ยวเนื่องสัมพันธ์กับบุคคลธรรมดาที่ถูกระบุ หรือสามารถถูกระบุอัตลักษณ์ได้ คือ บุคคลซึ่งสามารถถูกระบุอัตลักษณ์ได้ ไม่ว่าจะโดยตรงหรือโดยทางอ้อม โดยเฉพาะอย่างยิ่งด้วยการอ้างอิงถึงจากสิ่งที่ระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ สิ่งระบุอัตลักษณ์ออนไลน์หรือปัจจัยอย่างหนึ่ง หรือมากกว่านั้นที่เฉพาะเจาะจงไปยังอัตลักษณ์ทางกายภาพ กายวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น

[2] ISO/IEC 29100 : 2011 Informatiom technology-Security techiques Privacy Framework ข้อ 2.9 หมายถึง ข้อมูลที่ระบุตัวบุคคลได้ ติดต่อ หรือค้นหาตัวบุคคลหนึ่งหรือบุคคลใดโดยเฉพาะ หรือเป็นข้อมูลที่ใช้ร่วมกับข้อมูลอื่น เพื่อระบุตัวบุคคลหนึ่งบุคคลใดดังกล่าว มาจากคำ 4 คำในภาษาอังกฤษ คือ "ส่วนบุคคล" (Personal/Personally) "ระบุตัวตน" (identifying) "ระบุตัวตนได้" (identifiable)"

เราคงได้ยินตัวย่อ PDPA บ่อยมากๆ กันแล้วนะครับคำนี้ย่อมาจาก Personal Data Protection Act, B.E.2562 (2019) ขอเรียกว่า "PDPA 2019" แทนในบางบริบท หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางกรณีอาจใช้คำว่า "พระราชบัญญัตินี้" ก็ขอให้เข้าใจว่าเป็นกฎหมายฉบับเดียวกันนะครับ และจะขอเรียกว่า "พคข. 2562" แทนในบางบริบทเช่นเดียวกันนะครับ แน่นอนครับว่าส่งผลกระทบต่อผู้ประกอบกิจการในยุคมหาป่วน (Disruption) ดิจิทัล (Digital) พอสมควรเลยทีเดียว ทำให้ต้องมีมาตรฐานในการบริหารจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ เมื่อมีความจำเป็นต้องการขอใช้ข้อมูลส่วนบุคคลของใคร ก็จะต้องมีมาตรการป้องกันความเสี่ยงที่อาจจะมีผลกระทบไปถึงการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลซึ่งรู้จักกันดีว่า "CIA" นั่นเองครับ ซึ่งสำคัญมากทีเดียวเพราะอาจก่อให้เกิดแนวโน้มส่งผลกระทบในเชิงที่ไม่พึงประสงค์เสียหายในระดับบุคคลหรือองค์การได้เลยทีเดียว

ถ้าเราไปอ่านดูกฎหมาย พคข.2562/PDPA 2019 จะถูกเขียนไว้ก่อนเข้าสู่มาตราแรกว่า "โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา 26 ประกอบกับมาตรา 32 มาตรา 33 และมาตรา 37 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว" ถือว่าเป็นการอารัมภบทที่มาที่ไป และการให้ความสำคัญของการต้องมี พคข. 2562/PDPA 2019 ประกอบกับ ถ้าเราไปดูหมายเหตุท้ายสุดของกฎหมาย

ก็จะถึงบางอ้อว่าด้วยเหตุผลในการประกาศใช้ พคข. 2562/ PDPA2019 ที่ชัดเจนว่า "เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อน รำคาญ หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล (many cases of violations of the right to the privacy protection of personal data resulting in the nuisance to or damages to data subject)"

อีกทั้งเหตุผลที่เกิดจาก "ความก้าวหน้าทางเทคโนโลยีทำให้เกิดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ก.-ร.-ช.-ป.[3]/ CUD : Collection, Use, Disclosure) อันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็วก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป (General principles)"

ทั้งหมดข้างต้นนั้นเป็นเหตุผลว่าทำไมต้องให้ความสำคัญกับ PD/PII (ข้อมูลส่วนบุคคล) ยังไงล่ะครับ

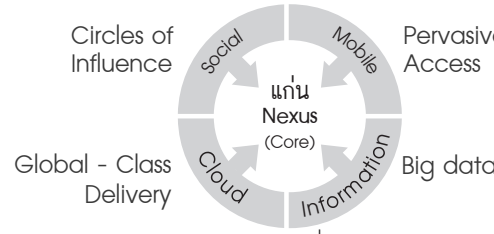
พคข.2562/PDPA 2019 มีด้วยกัน 96 มาตรา ซึ่งอาจารย์จะได้อธิบายในลำดับต่อไปอย่างละเอียดและเชื่อมโยงให้ค้นหากันง่าย ๆ

ก็เพราะ Thailand จะ 4.0 หรือ The 4th Industrial Revolution ด้วยกระมัง เพราะย้อนไปเมื่อหลายปีที่ผ่านมาโลกของเราอยู่ในยุคที่ 3 เรารู้จักกันดีว่า Information Age ยุคอินเทอร์เน็ต พอตอนนี้เรากำลังอยู่ในยุค Cyber Age มันก็เลยมีส่วนประกอบที่เรียกว่า The nexus of Disruptive Forces หรือ S'M'C'I[4] ขอเรียกว่า "4 Disruptive Forces"

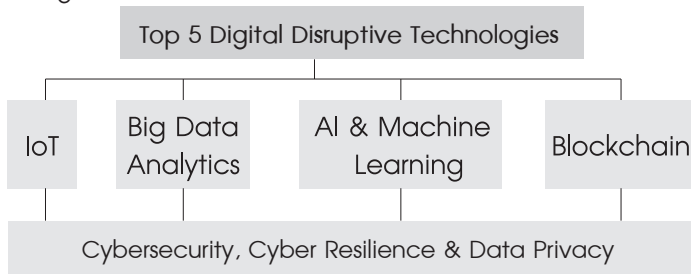
---

[3] *ก-เก็บ, ร.-รวบรวม, ช.-ใช้, ป.-เปิดเผย ซึ่งข้อมูลส่วนบุคคล โดยคำว่า ก.ร. จะใช้ติดกันว่าเก็บรวบรวม ไม่ได้แยกออกจากกันว่า เก็บเฉย ๆ เท่านั้น หากแต่ต้องรวบรวมมันด้วย จึงตรงกับคำว่า Collection นั่นเอง*

[4] *Social Mobile Cloud และ Informations แหล่งที่มา : Gartner*



ขณะเดียวกันโลกเกิดมหาป่วนเปลี่ยนแปลงด้านเทคโนโลยีขนานใหญ่ เกิด Disruptive Technology 5 ข้อใหญ่ๆ คือ IB_2AC[5] ขอเรียกว่า "5 Disruptive Technologies" ครับ



เมื่อพิจารณา Disruptive technology ลึกๆ ลงไปแล้ว เราเจอ Cybersecurity, Cyber Resilience และ Data Privacy มันคือรากฐานของ Disruptive Technology (Foundation) เลยก็ว่าได้

การเน้นที่ CCD[6] จึงเป็นที่มาของกฎหมายคู่แฝดคลอดออกมาปีเดียวกัน คือ 2562 ในส่วนของ Cybersecurity เรียกว่าพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ขอเรียกว่า พรซ.2562 แทนในบางบริบทโดยมี Cyber Resilience ไปรวมอยู่ด้วยกับ Data Privacy เรียกว่า พคข. 2562/PDPA 2019 นั่นเองครับ

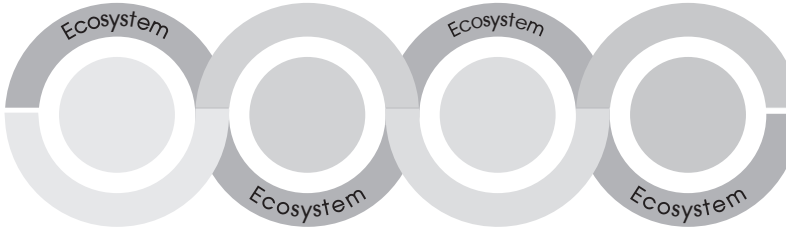
---

[5] *I = IoT (Internet of things), B_2 = Big Data Analytics และ Blockchain, A = AI (Artificial Intelligence หรือปัญญาประดิษฐ์) and Machine Learning, C = Cybersecurity, Cyber Resilience and Data Privacy, แหล่งที่มา : Top Five Disruptive Technologies ACIS Research*

[6] *Cybersecurity (การรักษาความมั่นคงปลอดภัยไซเบอร์) | Cyber Resilience (การรับมือภัยคุกคามไซเบอร์) | Data Privacy (ข้อมูลส่วนบุคคล)*

การปรับเปลี่ยนแปลงกายทางดิจิทัล (Digital Transformation) จำเป็นต้องเข้าใจแก่นแห่งสภาวะ Cyber[7] จากองค์ประกอบ 4 Disruptive Forces + 5 Disruptive Technologies เป็นเบื้องต้นก่อนเลย

"สภาวะไซเบอร์" ที่มี Internet เป็น Infrastructure (โครงสร้างพื้นฐาน) นั้น โลกปัจจุบันมีการเคลื่อนเปลี่ยนจาก Digital Economy ไปสู่ Data Economy ข้อมูลจึงเป็นยิ่งกว่าทองคำยังไงล่ะครับ และมันก็แปรเปลี่ยนจาก Data Economy ไปเป็น Crypto Economy และแล้วสภาวะท้ายที่สุดจะเปลี่ยนจาก Crypto Economy ไปสู่ Value Economy ในที่สุดครับ ขอเรียกสภาวะไซเบอร์อย่างนี้ว่า "The 4 Gen Economy"[8]



Digital Economy Data Economy Crypto Economy Value Economy

Disruptive Technology กับ Digital Transformation นั้น ถ้าเราหยุดนิ่งอยู่กับที่ ไม่คิดจะเปลี่ยนอะไรเลย เราจะถูกกระทบจาก Disruptive Technology เนื่องจากเทคโนโลยีใหม่ๆ มันอยู่รอบตัวเรา อย่างคนขับรถแท็กซี่ถูกคนขับรถส่วนตัวที่ร่วมมือกับ Grab ธนาคารถูก Banking 4.0 ส่งผลกระทบ ซึ่งมันไม่จำเป็นต้องไปธนาคาร มันอยู่ทุกที่ก็ว่าได้ รูปแบบใหม่ๆ ในการทำธุรกิจยุค Data Economy

---

[7] *พรซ.2562 มาตรา 3 Cyber (ไซเบอร์) หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป*

[8] *แหล่งที่มา : The 4 Gen Economy, ACIS research*

หรือ Sharing Economy ย่อมเกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ และข้อมูลส่วนบุคคลของคุณก็จะถูก ก.-ร.-ช.-ป. หรือ CUD ตามไปด้วย

โลกยุคดิจิทัล จึงไม่เป็นเพียงแค่เปลี่ยนรูปแบบ Digitization เช่น จากกระดาษเป็นคอมพิวเตอร์ จากอนาล็อกเป็นดิจิทัล จาก CD เป็น Drive ต่างๆ เท่านั้น แต่มันเป็นการ Digitalization คือ เอาเทคโนโลยีดิจิทัลไปใช้เปลี่ยน/ปรับรูปแบบในการทำมาค้าขาย หรือทำธุรกิจ เพื่อสร้างมูลค่าเพิ่มให้ลูกค้าปรับเปลี่ยนจริตเดิมๆ เพื่อมอบประสบการณ์ใหม่ๆ ให้ลูกค้าจากการเปลี่ยนรูปแบบนั้นๆ สร้างนวัตกรรม การบริหารจัดการที่เป็นเลิศด้านข้อมูล ต้องเข้าใจให้ได้เลยว่า Information หรือ Data เป็นสิ่งสำคัญมากขึ้นและมากขึ้น ทุกๆ คน ทุกๆ องค์กรล้วนต้องการ Information/Data ทั้งนั้น ส่วนเทคโนโลยี (Technology) เป็นเพียงเครื่องมือช่วยให้ง่าย อำนวยความสะดวก รวดเร็วในการจัดการกับ Information/Data ให้เกิด 2 ประสิทธิ คือ ประสิทธิภาพและประสิทธิผล ควบคู่กันไป และข้อสำคัญการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องไปด้วยกันกับการคุ้มครองข้อมูลส่วนบุคคลที่คำนึงถึงความเป็นส่วนตัวของเจ้าของข้อมูลด้วยนะครับ ถึงเวลาหรือยังที่ต้องแยก IT ออกมาเป็น I&T ให้ชัดเจนในการจัดการกับมันครับ

ภัยคุกคามไซเบอร์[9] (Cyber Threats) ที่ต้องการรับมือ (Cyber Resilience) นั้นมีมากขึ้นหลากหลายเดิมๆ ไม่ก็เปลี่ยนรูปแบบหรือมีใหม่ๆ ออกมาให้ผวากันไม่ว่าจะเป็นภัยคุกคามแบบไหนดังตัวอย่างต่อไปนี้ ก็ล้วนแล้วแต่เกี่ยวข้องกับความเป็นส่วนตัวและข้อมูลส่วนบุคคลของเราๆ ท่านๆ ทั้งสิ้นครับ

1. ภัยจากข้อมูลรั่วไหลออกไปจากการจัดเก็บข้อมูลในระบบคลาวด์

2. ภัยจากการโจมตีเจาะข้อมูลส่วนบุคคลในรูปแบบของ De-anonymization Attack

---

[9] *แหล่งที่มา : Top 10 cyber Threats and Trends 2019 (ข้อ 1-10) และ Top 10 cyber Threats 2020 (ข้อ11-20), Cybersecurity Prediction 2020*

3. ภัยจากการกลั่นแกล้ง หรือให้ร้ายป้ายสีทาง Social Media (Cyberbullying)

4. ภัยจากการเชื่อมต่ออุปกรณ์กับระบบอินเทอร์เน็ตโดยขาดความระมัดระวัง ทำให้เสี่ยงต่อการถูกโจมตีทางไซเบอร์

5. ภัยจากการนำเทคโนโลยี AI มาใช้ในด้านมืด

6. ภัยจากการทุจริตในการทำธุรกรรมทางอิเล็กทรอนิกส์

7. ภัยจากการที่องค์กรไม่สามารถปฏิบัติตามกฎหมายไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้

8. ภัยจากความเข้าใจผิดๆ ในธรรมชาติของ "สภาวะไซเบอร์"

9. ภัยจากความเข้าใจผิดในเรื่องของ Cryptocurrency และ Blockchain

10. ภัยจากความไม่เข้าใจของผู้บริหารระดับสูงในเรื่องของ Digital Transformation และ Cybersecurity Transformation

11. การโจมตีแบบฟิชชิ่งโดยใช้วิศวกรรมทางสังคม (Social Engineer) ขโมยข้อมูลผู้ใช้งานและโจมตีระบบคลาวด์

12. การรักษาความปลอดภัยของผู้ปฏิบัติงานด้วย Remote

13. การหลอกลวงบนคลาวด์ (Clound Jacking)

14. อุปกรณ์ IoT เติบโตจากการใช้งานและยังพบว่ามีภัยคุกคามต่อ IOMT (Internet of Medical Things) ที่อาจกลายเป็นวิกฤตด้านสุขภาพที่รุนแรง

15. การโจมตีของ Ransomware ที่ซับซ้อนและตรงเป้าหมายซึ่งโรงพยาบาลสระบุรีของไทยเราโดนเรียกค่าไถ่จากกรณีนี้ถึง 200,000 Bitcoin (63,000 ล้านบาท) เหตุเกิดเมื่อวันที่ 5 กันยายน 2563

16. Deep fakes ใช้ AI จัดการภาพหรือวิดีโอของบุคคลเพื่อแสดงอาชญากรรมบางอย่างที่ไม่ได้เกิดขึ้นจริง

17. มัลแวร์มือถือ

18. ช่องโหว่ความปลอดภัย 5G-to-WiFi

19. ภัยคุกคามจากภายในองค์การเอง เช่น การละเมิดข้อมูลส่วนบุคคล

20. ช่องโหว่และการละเมิดสิทธิ Application Programming Interface (API)

จากกรณีศึกษาที่เกิดขึ้นจริงต่อไปนี้ก็เป็นอีกเหตุผลหนึ่งที่ว่าทำไมต้องให้ความสำคัญ PDPA เช่น เหตุการณ์ในเดือนมิถุนายน 2560 ข้อมูลส่วนบุคคลผู้มีสิทธิออกเสียงเลือกตั้งของสหรัฐอเมริกาจำนวน 200 ล้านคนที่ Deep Root Analytics จัดเก็บเกิดรั่วไหล เนื่องจากไม่มีการตั้งรหัสที่ดีพอ ต่อมาในเดือนกรกฎาคม 2560 บริษัท Equifax ทำข้อมูลส่วนบุคคลของผู้บริโภคชาวอเมริกันรั่วไหลถึง 145 ล้านคน และในปีเดียวกันช่วงพฤศจิกายน 2560 Uber ทำข้อมูลส่วนบุคคลของคนขับรถและผู้ใช้บริการรั่วไหลถึง 53 ล้านคน

ปีต่อมา 2561 ในเดือนมกราคมระบบฐานข้อมูลของประชาชนชาวอินเดียตกเป็นข่าวว่ามีช่องโหว่ให้ผู้ที่ไม่หวังดีเข้าถึงข้อมูลของประชาชนกว่า 1 ล้านคน ได้โดยไม่ได้รับอนุญาต ต่อมาในเดือนมีนาคม 2561 Facebook ออกมายอมรับว่าดูแลข้อมูลส่วนบุคคลของผู้ใช้งานได้ไม่ดีพอ ทำให้ Cambridge Analytica นำข้อมูลผู้ใช้งานกว่า 50 ล้านคน ไปทำวิจัยแคมเปญหาเสียงเลือกตั้ง

เมษายน 2561 บ้านเราเองก็มีรายงานว่าข้อมูลของลูกค้าที่จัดเก็บไว้ในระบบ Cloud Amazon S3 รั่วไหล โดยผู้ไม่หวังดีสามารถเข้าถึงข้อมูลได้ 46,000 Files และในเดือนกรกฎาคม 2561 ธนาคารแห่งประเทศไทยคุมเข้มภัยไซเบอร์ เนื่องจากธนาคารกสิกรไทยและธนาคารกรุงไทยถูกมือดีแฮกข้อมูล

<u>กรณีศึกษาค่าปรับสูงที่สุดในประวัติศาสตร์โลก</u> จากการที่ Facebook ทำรายได้มากถึง 55,000 ล้านดอลลาร์สหรัฐ ในปี ค.ศ. 2018 (พ.ศ. 2561) แต่ทว่าโดน FTC[10] (Federal Trade Commission) ปรับกรณีละเมิดสิทธิความเป็นส่วนตัว

---

[10] *หน่วยงานหลักที่บริหารควบคุมกิจกรรมต่าง ๆ ในพาณิชย์อิเล็กทรอนิกส์*

ของผู้ใช้งานประมาณ 5,000 กว่าล้านดอลลาร์สหรัฐ คิดเป็น 10% ของรายได้ทั้งหมด จากกรณีแชร์ข้อมูลส่วนบุคคลของผู้ใช้งานกว่า 50 ล้านคน ให้กับบริษัท CA[11] ประมวลและวิเคราะห์ความคิดเห็นของประชาชนด้านการเมือง โดยที่ไม่ได้ขอความยินยอมจากผู้ใช้งานแม้แต่น้อย

กรณีศึกษาค่าปรับสูงที่สุดในประวัติศาสตร์ของ GDPR จากกรณีศึกษาจริงของ Google ทำรายได้ในปี 2018 (พ.ศ. 2561) ปีเดียวกับกรณีศึกษาของ Facebook แต่โดนเรียกปรับประมาณ 300 ล้านดอลลาร์สหรัฐ คิดเป็น 1.5% ของรายได้ เกิดจากการละเมิดหลายเคสมาก แต่ที่โด่งดังก็คือ การประมวลผลข้อมูลของผู้เยาว์เพื่อทำการขายโฆษณาแบบเจาะจง (Re-targeting Ad) ซึ่งมิได้ขอความยินยอมจากผู้ปกครอง และอีกหลายต่อหลายเคสคือ การทำ Consent (ความยินยอม) แบบแอบซ่อนไม่ชัดเจนตอนบอกรับสมัครสมาชิก Google Account ซึ่งต้องให้ผู้ใช้งานกดหลายขั้นตอนและได้นำข้อมูลไปทำ Personalized Advertisement[12]

กรณีศึกษาค่าปรับสูงที่สุดในประวัติศาสตร์ ICO[13] จากกรณี British Airways

---

[11] *CA : Cambridge Analytica ซึ่งกรณีเรื่องจริงนี้ Netflix ได้นำมาทำเป็นสารคดีดีแง่ด้านมืดของการนำข้อมูลส่วนบุคคลไปใช้ในภาพยนตร์แฮ็ก (แหกตา) สนั่นโลก (The Great Hack) ทำให้เกิดสมการใหม่ว่า Behavior Change = Behavioral psychology + Big Data + Targeted Engagement ซึ่งเป็นการเปลี่ยนแปลงพฤติกรรมไปตามจิตวิทยาพฤติกรรม โดยนำข้อมูลขนาดใหญ่ที่เก็บรวบรวม ประมวลผลของเจ้าของข้อมูลส่วนบุคคลมายำให้บิดเบือน ทำให้ชักนำให้เข้าไปมีส่วนร่วมในเป้าหมายที่ถูกกำหนดไว้อย่างง่ายดาย*

[12] *เป็นการทำการตลาดส่วนบุคคลหรือจะเรียกว่า One to One Marketing เป็นแนวคิดและวิธีการที่นักการตลาดพยายามนำเสนอสินค้าและบริการให้ตรงใจของผู้บริโภคให้มากที่สุด โดยไม่มีความจำเป็นต้องนำเสนอสินค้าอย่างเดียวกันนั้นให้กับทุกคน แต่จะมุ่งเน้นเจาะจงไปที่ความต้องการอย่างแท้จริง หรือความสนใจของลูกค้าแต่ละคน หรือกลุ่มลูกค้าผู้บริโภค และบางครั้งจะพิจารณาจากพฤติกรรมของลูกค้าเป็นสำคัญ ด้วยอย่างเดียวกันกับการทำ Retargeting หรือ Remarketing โดยติดตามลูกค้าที่เข้าชมเว็บไซต์ดูสินค้าชนิดหนึ่งแต่ยังไม่ตัดสินใจซื้อ เมื่อลูกค้าออกจากเว็บไซต์ แต่ไปเข้าเว็บไซต์อื่น ลูกค้าจะถูกติดตามด้วยเทคนิคที่เรียกว่า Retargeting โดยจะเห็น Banner Ads. ของแบรนด์ติดตามไปตลอดทุกเว็บไซต์ที่ลูกค้าไปเยือน เพื่อเป็นการตอกย้ำและกระตุ้นให้เกิดการตัดสินใจซื้อ*

[13] *Information Commissioner's Office คณะกรรมาธิการสารสนเทศแห่งสหราชอาณาจักร*

ถูกเจาะระบบข้อมูลทำให้ข้อมูลลูกค้ากว่า 500,000 คน ถูกขโมยไปจากการ Hack เว็บไซต์ คล้ายๆ Phishing ข้อมูลที่ถูกขโมยได้แก่ ชื่อ ที่อยู่ อีเมล และข้อมูลการชำระเงินในปี 2018 (พ.ศ. 2561) British Airways ทำรายได้ 13,000 ล้านปอนด์ แต่ถูกปรับถึง 204 ล้านปอนด์ หรือคิดเป็นประมาณ 1% ของรายได้

นอกจากนั้นแล้วโรงแรม Marriott International เครือโรงแรม W, Westin, Le Meridien และ Sheraton ถูกปรับจาก GDPR ถึง 99.2 ล้านปอนด์ เนื่องจากข้อมูลส่วนบุคคลรวมถึงรายละเอียดบัตรเครดิต หมายเลขพาสปอร์ต และวันเดือนปีเกิดของลูกค้ากว่า 339 ล้านคน ได้ถูก Hack ไป

กรณีศึกษาประเทศสิงคโปร์ มีการบังคับใช้กฎหมาย PDPA กว่า 10 ปี มีการเพิ่มความเข้มงวดมากยิ่งขึ้น เนื่องจากระบบเทคโนโลยีสารสนเทศของ SingHealth[14] ถูก Hack ส่งผลให้ข้อมูลผู้เข้ารับการรักษาในโรงพยาบาลและคลินิกในเครือ 1,500,000 คน ถูกขโมยออกไป ข้อมูลที่ว่านั้น ได้แก่ ชื่อ ที่อยู่ เพศ สัญชาติ วันเกิด และหมายเลขบัตรประจำตัวประชาชน

ข้อมูลการจ่ายยาผู้ป่วยนอกประมาณ 160,000 ราย ได้ถูกขโมยไป หนึ่งในนั้นคือข้อมูลของ Lee Hsien Loong นายกรัฐมนตรีคนปัจจุบันของสิงคโปร์ ค่าปรับจากคดีนี้สูงถึง 1 ล้านดอลลาร์สิงคโปร์ครับ

ในปี2019 (พ.ศ. 2562) มียอดการปรับรวมสูงถึง 1.54 ล้านดอลลาร์สิงคโปร์สูงสุดในประวัติศาสตร์ของประเทศสิงคโปร์ สูงกว่า 3 ปีก่อน (ค.ศ. 2016-2018, พ.ศ. 2559 - 2561) รวมกันเกือบ 5 เท่า และกว่า 100 องค์การที่โดนปรับมาจากทุกอุตสาหกรรม โดยเฉพาะค้าปลีก การเงิน วิชาชีพเฉพาะทาง เช่น แพทย์ ส่วนหนึ่งมาจากการมีระบบปกป้องข้อมูลที่ไม่ถูกต้องตามมาตรฐาน และยังพบในองค์กรการกุศลอีกถึง 10 แห่ง ที่มีความผิดและโดนปรับด้วยครับ

---

[14] *เป็นเครือหน่วยงานด้านสาธารณสุขที่ใหญ่ที่สุดในประเทศสิงคโปร์ ประกอบด้วย 2 โรงพยาบาลใหญ่ 5 คลินิกพิเศษ และโพลีคลินิกรวม 8 แห่ง*

มาตรการลงโทษ

• ถ้าเป็น GDPR ของทางสหภาพยุโรป มีปรับสูงสุด 20 ล้านยูโร หรือ 4% ของรายได้รวมทั้งปีของธุรกิจ แล้วแต่ว่าจำนวนใดจะมากกว่า (ประมาณ 735 ล้านบาทไทย)

• PDPA ของสิงคโปร์ปรับสูงสุด 1 ล้านดอลลาร์สิงคโปร์ (ประมาณ 22.85 ล้านบาทไทย)

• PDPA ของมาเลเซีย ปรับสูงสุด 500,000 ริงกิต (ประมาณ 3 ล้านบาทไทย)

• PDPA ของประเทศไทยถือว่ารุนแรงกว่า เนื่องจากมีโทษจำคุกด้วยและมีเป็น 3 ลักษณะโทษ (รวม 14 มาตรา)

อ้างอิง พคข. 2562/ PDPA 2019 หมวด 6 ความรับผิดทางแพ่งมาตรา 77 ถึงมาตรา 78 (2 มาตรา) หมวด 7 บทกำหนดโทษ ส่วนที่ 1 โทษอาญา มาตรา 79 ถึงมาตรา 81 (3 มาตรา) ส่วนที่ 2 โทษทางปกครองมาตรา 82 ถึงมาตรา 90 (9 มาตรา) จึงขออธิบายไว้ก่อนเลย ดังนี้

1. ความรับผิดทางแพ่ง (พคข.2562/PDPA 2019 มาตรา 77)

1.1 ผู้ควบคุมข้อมูลส่วนบุคคล[15] หรือผู้ประมวลผลข้อมูลส่วนบุคคล[16] ซึ่งดำเนินการใด ๆ หรืออะไรก็ตามที่เกี่ยวข้องสัมพันธ์กันกับ PD[17] อันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตาม พคข.2562/PDPA 2019 ไม่ว่าจะมาตราไหนก็ตาม

---

[15] ถ้าเป็น Alternative term ใช้คำว่า Controller หรือเต็มยศหน่อยก็จะเป็น Personal ; Data Controller ส่วน Terms as used in ISO/IEC27701 จะใช้คำว่า PII Controller ซึ่งทราบกันดีอยู่แล้วว่า PII คือ Personally Identifiable Information ที่ตรงกับ Alternative term คือ Personal Data (ข้อมูลส่วนบุคคล) ของประเทศไทยนั่นเองครับ

[16] Alternative term คือ Processer หรือ Personal data Processer แต่ถ้าเป็น ISO/IEC27701 ใช้ว่า PII processor

[17] Personal Data (ข้อมูลส่วนบุคคล) หรือ PII ถือว่าเป็นความหมายเดียวกัน อาจย่อว่า "PD" ก็ได้

1.2 ผลที่ตามมาทำให้เกิดความเสียหายต่อ DS[18]

1.3 Controller หรือ Processor นั้นต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่ DS ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม ดังนั้น หากจะพ้นผิดไม่ต้องชดใช้ค่าสินไหมทดแทนก็ต้องพิสูจน์ตนเองว่า ไม่ได้จงใจหรือไม่ได้ประมาทเลินเล่อเท่านั้นครับ เช่น ใช้ความระมัดระวังเต็มที่สุดๆ แล้ว ไม่ใช่แค่กล่าวอ้างลอยๆ ต้องมีหลักฐานเชิงประจักษ์(OE : Objective Evidence) มารองรับด้วย จึงจะรอด หรือไม่ก็เข้าข้อยกเว้นในข้อ 1.4 ต่อไปนี้เท่านั้นครับ

1.4 มีข้อยกเว้น ว่าถ้า Controller[19] หรือ Processor[20] นั้นจะพิสูจน์ได้ว่า

1.4.1 ความเสียหายนั้นเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้น(ไม่กระทำ) ของ DS เอง คือ DS มีหน้าที่รับผิดชอบต้องขยัน Backup ข้อมูล แต่คุณไม่ทำอย่างนี้ Controller/Processor ไม่มีความผิดครับ (พคข.2562/PDPA 2019 มาตรา 77 (1))

1.4.2 เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย (พคข.2562/PDPA 2019 มาตรา 77 (2)) เช่น เจ้าพนักงานบังคับคดีหรือศาลมีหมายขอข้อมูลส่วนบุคคลที่ Controller มีอยู่ เป็นต้น

---

[18] Data Subject (เจ้าของข้อมูลส่วนบุคคล) หรือ PII Principal อาจย่อว่า "DS" ก็ได้

[19] "ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่าบุคคล[21] หรือนิติบุคคลซึ่งมีอำนาจหน้าที่ ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล (พคข.2562/PDPA 2019 มาตรา 6) อาจย่อว่า "DC" ก็ได้

[20] "ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (ตรงนี้มีประเด็นซึ่งจะอธิบายต่อไป) (พคข.2562/PDPA 2019 มาตรา 6) อาจย่อว่า "DP" ก็ได้

[21] "บุคคล" หมายความว่าบุคคลธรรมดา (พคข.2562/PDPA 2019 มาตรา 6)

1.5 กรณีต้องขดใช้ "ค่าสินไหมทดแทน" แบ่งออกเป็น 2 กรณี ดังต่อไปนี้

1.5.1 ค่าสินไหมทดแทนที่แท้จริง (จ่ายไปตามจริง) ตาม พคข.2562/ PDPA 2019 มาตรา 77 วรรค 2 ว่าค่าสินไหมทดแทนให้หมายความรวมถึง ค่าใช้จ่ายทั้งหมด ที่ DS ได้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น (คือยังไม่เกิดขึ้น แต่แนวโน้มมันส่อจะเสียหายจึงขอป้องกันไว้ก่อน แต่ต้องไม่ใช่วิตกจริตกังวลจนเกินไปนะครับ) หรือได้ใช้จ่ายไปเพื่อระงับความเสียหายที่เกิดขึ้นแล้วเป็นที่เรียบร้อย

1.5.2 ค่าสินไหมทดแทนเพื่อการลงโทษ ปรากฏใน พคข.2562/ PDPA 2019 มาตรา 78 ว่าให้ศาลท่านมีอำนาจในการสั่งให้ Controller หรือ Processor จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงตามข้อ 1.5.1 ข้างต้นโดยให้ขึ้นอยู่กับดุลพินิจของศาลที่จะกำหนดให้ตามที่เห็นสมควร แต่ทว่าห้ามเกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริงด้วยนะครับ

1.6 ค่าสินไหมทดแทนเพื่อการลงโทษ เป็นอำนาจของศาลก็จริง แต่ต้องเป็นไปตามหลักเกณฑ์ต่อไปนี้ ประกอบการใช้ดุลพินิจด้วยนะครับ (พคข.2562/ PDPA 2019 มาตรา 78 วรรค 1)

1.6.1 ความร้ายแรงของความเสียหายที่ DS ได้รับ

1.6.2 ผลประโยชน์ที่ Controller หรือ Processor ได้รับ

1.6.3 สถานะทางการเงินของ Controller หรือ Processor

1.6.4 การที่ Controller หรือ Processor ได้บรรเทาความเสียหายที่เกิดขึ้น

1.6.5 การที่ DS ก็มีส่วนในการก่อให้เกิดความเสียหายดังกล่าวนั้นด้วยเช่นกัน ซึ่ง"เกณฑ์ประกอบการใช้ดุลพินิจของศาล" ข้างต้นนี้เรียกว่า "5 พฤติการณ์ที่พึงคำนึงในการใช้ดุลพินิจนั่นเอง"

1.7 อายุความเรียกร้อง พคข.2562/PDPA 2019 มาตรา 78 วรรค 2 บัญญัติสิทธิในการเรียกร้องค่าเสียหายอันเกิดจากการละเมิด PD (ข้อมูลส่วนบุคคล) ตามกฎหมายทุกกรณี เป็นอันขาดอายุความเมื่อพ้น 3 ปี นับแต่วันที่ผู้เสียหาย (ใครก็ได้ที่เสียหายไม่เฉพาะ DS เท่านั้น) รู้ถึงความเสียหายและรู้ตัว Controller หรือ Processor ที่ต้องรับผิด ฉะนั้น ถ้ารู้ความเสียหาย แต่ยังไม่รู้เลยว่าใครทำให้เสียหาย อายุความยังไม่เริ่มนับนะ หรือยังไม่รู้ว่าตัวเองเสียหาย แต่รู้ว่า Controller /Processor เป็นใครก็ยังไม่มีอำนาจในการเรียกร้องหรือขาดอายุความเมื่อพ้น 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล กรณีนี้อายุความเรียกร้องกฎหมายขยายให้เต็มที่ แต่ห้ามเกิน 10 ปี ในการรู้ถึงความเสียหาย รู้ตัว Controller/Processor ที่ทำให้เสียหายและต้องรับผิด

2. โทษอาญา (พคข.2562/PDPA 2019 มาตรา 79)

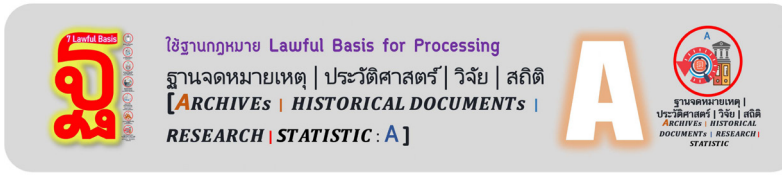
2.1 Controller ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนดไว้ดังนี้

2.1.1 ฝ่าฝืนมาตรา 27 วรรค 1 หรือ วรรค 2

มาตรา 27 วรรค 1 กฎหมายห้ามมิให้ Controller ใช้หรือเปิดเผยข้อมูลส่วนบุคคล (คือจะไม่รวมถึงการเก็บรวบรวมนะครับ) โดยไม่ได้รับความยินยอมจาก DS เว้นแต่

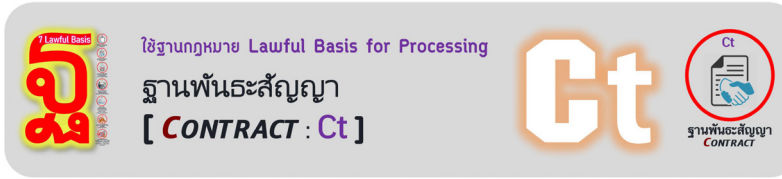
2.1.1.1 เป็น PD ที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (เป็น PD ประเภท GPD : General Personal Data) ได้แก่

- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งจัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิเสรีภาพของ DS ทั้งนี้ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด (พคข.2562/PDPA 2019 มาตรา 24 (1))
- โดยใช้ฐานกฎหมาย "ฐ" (Lawful Basis) ต่อไปนี้ในการประมวลผลข้อมูลส่วนบุคคล

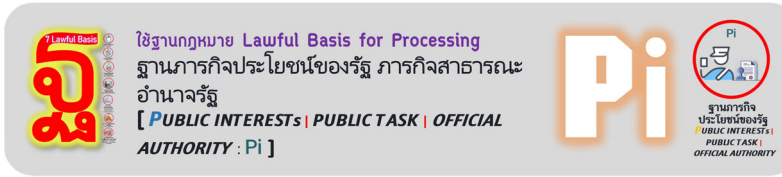


• เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (พคข.2562/PDPA 2019 มาตรา 24 (2))

• เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่ง DS เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของ DS ก่อนเข้าทำสัญญานั้น (รวมข้อตกลงด้วย) (พคข.2562/PDPA 2019 มาตรา 24 (3))



• เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินธุรกิจเพื่อประโยชน์สาธารณะของ Controller หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล (พคข.2562/PDPA 2019 มาตรา 24 (4))



- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของ Controller หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของ DS (พคข.2562/PDPA 2019 มาตรา 24 (5))

- เป็นการปฏิบัติตามกฎหมายของ Controller (พคข.2562/PDPA 2019 มาตรา 24 (6))

2.1.1.2 เป็น PD ที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 26 (เป็น PD ประเภท SPD : Sensitive Personal Data) ได้แก่ กรณีข้อมูลส่วนบุคคลที่อ่อนไหว กฎหมายจะห้ามมิให้เก็บรวบรวม PD ดังต่อไปนี้

1. เชื้อชาติ (สัญชาติไม่ถือเป็น SPD)
2. เผ่าพันธุ์
3. ความคิดเห็นทางการเมือง
4. ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
5. พฤติกรรมทางเพศ
6. ประวัติอาชญากรรม
7. ข้อมูลสุขภาพ ความพิการ