

PDPA สำหรับธุรกิจ: ฐานการประมวลผล สิทธิเจ้าของข้อมูล และโทษที่เจ้าของกิจการต้องรู้

โดย เอกสยาม ชัยศรี ที่ปรึกษากฎหมาย
บริษัท เอกสยาม แอนด์ पार्टเนอร์ส จำกัด

เนื้อหานี้เป็นข้อมูล กฎหมายทั่วไป ไม่ใช่ความเห็นทางกฎหมายเฉพาะกรณี การพิจารณาแต่ละเรื่อง ต้องอาศัย
ข้อเท็จจริงและพยานหลักฐานของเรื่องนั้น ฉบับออนไลน์ที่ปรับปรุงล่าสุดอยู่ที่ [https://
eksiamcorporatelaw.com/articles/pdpa-guide.html](https://eksiamcorporatelaw.com/articles/pdpa-guide.html)

กฎหมายที่ใช้อ้างอิงในบทความนี้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: *กฎหมายหลัก (PDPA)*
- มาตรา 6 นิยามข้อมูลส่วนบุคคล และมาตรา 26 ข้อมูลส่วนบุคคลอ่อนไหว: *ข้อมูลที่ต้องระวังเป็นพิเศษ*
- มาตรา 19 และมาตรา 24 ว่าด้วยความยินยอมและฐานทางกฎหมายอีก 6 ประการ: *หัวใจของ PDPA*
- มาตรา 19 มาตรา 23 และมาตรา 30-36 ว่าด้วยสิทธิของเจ้าของข้อมูลส่วนบุคคล: *สิทธิที่ธุรกิจต้องรองรับ*
- มาตรา 77-90 ว่าด้วยความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครอง: *ผลของการฝ่าฝืน*

PDPA คืออะไร และใครต้องปฏิบัติตาม?

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่รู้จักกันในชื่อ "PDPA" (Personal Data Protection Act) มีผลบังคับใช้เต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน 2565 กฎหมายนี้ใช้บังคับกับ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ทุกฝ่าย ไม่ว่าจะเป็นบริษัท ห้างหุ้นส่วน หรือบุคคลธรรมดาที่เก็บรวบรวมหรือใช้ข้อมูลส่วนบุคคลของบุคคลอื่น

กฎหมายให้นิยามสำคัญไว้ในมาตรา 6 ว่า



"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ"

: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6

ในทางปฏิบัติ "ข้อมูลส่วนบุคคล" ครอบคลุมสิ่งที่ธุรกิจทุกขนาดเก็บอยู่แล้วในชีวิตประจำวัน ไม่ว่าจะเป็น ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมล ที่อยู่ IP address รูปภาพใบหน้า ข้อมูลทางการแพทย์ หรือ แม้กระทั่งคุกกี้ที่ติดตามพฤติกรรมบนเว็บไซต์

ข้อมูลส่วนบุคคลอ่อนไหว: ต้องระวังเป็นพิเศษ

กฎหมายแบ่งข้อมูลส่วนบุคคลออกเป็นสองระดับ โดย "ข้อมูลส่วนบุคคลอ่อนไหว" (Sensitive Personal Data) ตามมาตรา 26 ต้องการการคุ้มครองสูงกว่าปกติ และห้ามประมวลผลโดยปราศจากความยินยอมโดยชัดแจ้ง (Explicit Consent) เว้นแต่จะเข้าข้อยกเว้นที่กฎหมายกำหนด ข้อมูลอ่อนไหวได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม และข้อมูลชีวภาพ (ลายนิ้วมือ ใบหน้า)

ฐานทางกฎหมาย 7 ประการที่ต้องมีก่อนประมวลผลข้อมูล

หัวใจสำคัญที่สุดของ PDPA คือ การประมวลผลข้อมูลส่วนบุคคลทุกครั้งต้องมี "ฐานทางกฎหมาย" รองรับ ฐานแรกคือความยินยอมตามมาตรา 19 และมาตรา 24 กำหนดฐานที่เก็บรวบรวมได้โดยไม่ต้องขอความยินยอมอีก 6 ประการ รวมเป็น 7 ฐาน

"ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้"

: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

ฐานทั้ง 7 ประการ ได้แก่



ฐาน	เงื่อนไข	ตัวอย่างการใช้งาน
1. ความยินยอม (Consent)	เจ้าของข้อมูลยินยอมโดยสมัครใจ ชัดเจน ถอนได้	การสมัคร Newsletter การรับโปรโมชั่น
2. สัญญา (Contract)	จำเป็นต้องใช้ข้อมูลเพื่อปฏิบัติตามสัญญา	ส่งสินค้าถึงบ้าน เบิกเงินเดือนพนักงาน
3. หน้าที่ตามกฎหมาย (Legal Obligation)	กฎหมายกำหนดให้ต้องเก็บหรือเปิดเผย	ยื่นภาษีต่อสรรพากร ส่งข้อมูลประกันสังคม
4. ประโยชน์สำคัญต่อชีวิต (Vital Interest)	จำเป็นเพื่อป้องกันอันตรายต่อชีวิตหรือสุขภาพ	เหตุฉุกเฉินทางการแพทย์
5. การกิจสาธารณะหรือการใช้อำนาจรัฐ (Public Task)	จำเป็นเพื่อดำเนินการกิจเพื่อประโยชน์สาธารณะ หรือใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูล	หน่วยงานที่ได้รับมอบอำนาจรัฐตามกฎหมาย
6. จดหมายเหตุ วิจัย หรือสถิติ (Archives, Research or Statistics)	เพื่อจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัย หรือสถิติ โดยมีมาตรการปกป้องที่เหมาะสม	งานวิจัย สถิติสาธารณสุข
7. ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)	จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์นั้นมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูล	ป้องกันการฉ้อโกง วิเคราะห์ข้อมูลลูกค้าเพื่อปรับปรุงบริการ

ข้อผิดพลาดที่พบบ่อยคือธุรกิจอาศัยฐาน "ความยินยอม" เป็นฐานเดียวสำหรับทุกกิจกรรม ทั้งที่ในหลายกรณีฐาน "สัญญา" หรือ "ประโยชน์อันชอบธรรม" อาจเหมาะสมกว่า เพราะฐานความยินยอมมีข้อเสียคือเจ้าของข้อมูลสามารถถอนความยินยอมได้ทุกเมื่อ ซึ่งทำให้ธุรกิจต้องหยุดประมวลผลข้อมูลนั้น



สิทธิ 8 ประการของเจ้าของข้อมูลที่ธุรกิจต้องรองรับ

กฎหมาย PDPA มอบสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคล 8 ประการ ซึ่งผู้ควบคุมข้อมูลต้องมีระบบรองรับคำขอใช้สิทธิเหล่านี้อย่างเป็นระบบ (สำหรับคำขอเข้าถึงข้อมูล ต้องดำเนินการโดยไม่ชักช้าและไม่เกิน 30 วัน นับแต่วันที่ได้รับคำขอ ตามมาตรา 30) ได้แก่ สิทธิรับทราบ (Right to be Informed), สิทธิขอเข้าถึงข้อมูล (Right of Access), สิทธิขอแก้ไขข้อมูล (Right to Rectification), สิทธิขอลบข้อมูล (Right to Erasure), สิทธิขอระงับการใช้ข้อมูล (Right to Restriction), สิทธิขอรับข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Right to Data Portability), สิทธิคัดค้านการประมวลผล (Right to Object) และสิทธิถอนความยินยอม (Right to Withdraw Consent)

บทบาท DPO: ต้องแต่งตั้งหรือไม่?

กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลบางประเภทต้องแต่งตั้ง "เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" หรือ DPO (Data Protection Officer) ตามมาตรา 41 ซึ่งได้แก่ หน่วยงานรัฐ ผู้ควบคุมข้อมูลที่ต้องเฝ้าระวังเจ้าของข้อมูลในวงกว้างเป็นประจำ หรือผู้ที่ประมวลผลข้อมูลอ่อนไหวเป็นกิจกรรมหลัก สำหรับธุรกิจขนาดกลาง-เล็กทั่วไปที่ไม่ได้อยู่ในข่ายดังกล่าว การแต่งตั้ง DPO ไม่ใช่ข้อบังคับ แต่การมีผู้รับผิดชอบด้าน PDPA ภายในองค์กรยังคงเป็นแนวปฏิบัติที่ดี

โทษทางปกครองและโทษอาญา

กฎหมาย PDPA กำหนดโทษไว้สองระดับ ซึ่งมีผลกระทบร้ายแรงต่อธุรกิจที่ฝ่าฝืน

"ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท"

: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 84



ประเภทโทษ	ฐานความผิด	อัตราโทษสูงสุด
โทษปกครอง	ไม่แจ้งรายละเอียดตามมาตรา 23 (Privacy Notice) / ไม่ดำเนินการตามคำขอเข้าถึงข้อมูลภายในกำหนด / ไม่จัดให้มี DPO เมื่อกฎหมายกำหนด (มาตรา 82)	1 ล้านบาท
โทษปกครอง	เก็บ/ใช้/เปิดเผยข้อมูลโดยไม่มีฐานทางกฎหมาย / ส่งข้อมูลไปต่างประเทศโดยไม่เป็นไปตามมาตรา 28 หรือ 29 (มาตรา 83)	3 ล้านบาท
โทษปกครอง	เก็บ/ใช้/เปิดเผยข้อมูลอ่อนไหวโดยไม่ชอบ / ส่งข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบ (มาตรา 84)	5 ล้านบาท
โทษอาญา	ใช้หรือเปิดเผยข้อมูลอ่อนไหวโดยมิชอบ หรือส่งไปต่างประเทศโดยไม่เป็นไปตามมาตรา 28 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย (มาตรา 79 วรรคหนึ่ง)	จำคุกไม่เกิน 6 เดือน / ปรับไม่เกิน 5 แสนบาท
โทษอาญา	การกระทำความผิดด้วยกันเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น (มาตรา 79 วรรคสอง)	จำคุกไม่เกิน 1 ปี / ปรับไม่เกิน 1 ล้านบาท

ขั้นตอนที่ธุรกิจต้องทำเพื่อให้สอดคล้องกับ PDPA

ธุรกิจที่ต้องการให้การดำเนินงานสอดคล้องกับ PDPA ควรเริ่มต้นด้วยการทำ Data Mapping หรือสำรวจว่าองค์กรเก็บข้อมูลส่วนบุคคลอะไรบ้าง จากแหล่งใด ใช้เพื่อวัตถุประสงค์ใด และเก็บรักษาไว้นานเพียงใด จากนั้นจัดทำ Privacy Notice หรือนโยบายความเป็นส่วนตัวที่ครอบคลุม พร้อมสร้างกระบวนการรับคำขอใช้สิทธิจากเจ้าของข้อมูล และฝึกอบรมพนักงานให้เข้าใจหน้าที่ตามกฎหมาย

สิ่งที่ธุรกิจควรตรวจสอบทันที

- เว็บไซต์มีนโยบายความเป็นส่วนตัว (Privacy Policy) ที่ถูกต้องหรือไม่?
- แบบฟอร์มออนไลน์มีกล่อง Consent ที่ไม่ได้ติ๊กไว้ล่วงหน้าหรือไม่?
- มีกระบวนการรับเรื่องและตอบสนองคำขอเจ้าของข้อมูลภายใน 30 วันหรือไม่?
- ข้อมูลพนักงาน ลูกค้า และคู่ค้ามีการจัดเก็บอย่างปลอดภัยหรือไม่?
- สัญญากับผู้ประมวลผลข้อมูลภายนอก (Cloud, HR System) มี DPA (Data Processing Agreement) หรือไม่?



ทำไมธุรกิจถึงต้องการที่ปรึกษา PDPA?

ความซับซ้อนของ PDPA ไม่ได้อยู่ที่ตัวกฎหมายเพียงอย่างเดียว แต่อยู่ที่การนำหลักการไปปรับใช้กับกิจกรรมทางธุรกิจจริง ซึ่งมีความหลากหลายและเปลี่ยนแปลงตลอดเวลา เอกสยาม ชัยศรี ที่ปรึกษากฎหมาย ซึ่งมีขอบเขตงานครอบคลุม กฎหมายเทคโนโลยี และการคุ้มครองข้อมูลส่วนบุคคล ให้คำปรึกษา โดยพิจารณาทั้งตัวบทและกิจกรรมทางธุรกิจของแต่ละองค์กรไปพร้อมกัน และช่วยจัดทำ Privacy Policy, Consent Form, Data Processing Agreement และ Record of Processing Activities (RoPA) ที่ใช้งานได้จริงและสอดคล้องกับกฎหมาย

สรุปสาระสำคัญ

- PDPA ใช้บังคับกับทุกธุรกิจที่เก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าขนาดใด
- การประมวลผลต้องมีฐานทางกฎหมาย 1 ใน 7 ประการ (ความยินยอม หรือฐานตามมาตรา 24) ไม่ใช่แค่ "ขอความยินยอม" เสมอไป
- ข้อมูลอ่อนไหว (สุขภาพ ชีวภาพ ศาสนา ฯลฯ) ต้องการมาตรการคุ้มครองที่เข้มข้นกว่า
- เจ้าของข้อมูลมีสิทธิ 8 ประการที่ธุรกิจต้องรองรับ โดยคำขอเข้าถึงข้อมูลต้องดำเนินการภายใน 30 วัน
- โทษปรับทางปกครองสูงสุด 5 ล้านบาท และโทษอาญาจำคุกไม่เกิน 1 ปี

