กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Personal Data Protection Act (PDPA)

ข้อมูลส่วนบุคคลคืออะไร (Personal Data)

ข้อเท็จจริงใด ๆ ที่สามารถระบุหรือยืนยันความเป็นตัวบุคคลไม่ว่าจะเป็นทางตรงหรือทางอ้อม เช่น ชื่อ วันเกิด ที่อยู่ อีเมล์ หมายเลขโทรศัพท์ ข้อมูลบัตรเครดิต เป็นต้น

ข้อมูลส่วนบุคคลมีความเสี่ยงอย่างไร?

- ถูกขโมยตัวตน เพื่อใช้ก่ออาชญากรรม (Identity Theft)
- การประมวลผลข้อมูล เพื่อใช้กำหนด Profile ในการแสวงหาประโยชน์ (Profiling)
- การขายข้อมูล เพื่อใช้ประโยชน์ทางการตลาด (Misuse)
- การถูกติดตามหรือถูกสอดแนม (Tracking / Stalking)

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

พฤศจิกายน 2560

บริษัท Uber ข้อมูลส่วนบุคคลของคนขับรถ และ ผู้ใช้บริการ รั่วไหล 53 ล้านคน

มกราคม 2561

ระบบฐานข้อมูลประชาชนของอินเดียกว่า 1,000 ล้านคน ถูกเข้าถึงโดยไม่ได้รับอนุญาตจากผู้ไม่ประสงค์ดี

กรกฎาคม 2562

Facebook ถูกปรับ 1.55 แสนล้านบาท เหตุจากไม่สามารถปกป้องข้อมูลผู้ใช้งานได้ จนทำให้ Cambridge Analytica นำข้อมูล user กว่า 50 ล้านคน ไปทำวิจัยหาเสียงเลือกตั้ง

ความสำคัญของ PDPA

- เพื่อใช้ในการป้องกันข้อมูลส่วนบุคคลจากการเก็บรวบรวม ใช้ เปิดเผยผิดวัตถุประสงค์ โดยมีกลไกจัดการข้อมูลส่วนบุคคลที่เหมาะสม

- เพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครอง สามารถตรวจสอบและควบคุมผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน

- เพื่อสร้างความเชื่อมั่นให้แก่นานาชาติว่าประเทศไทยมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปที่เพียงพอ

- อำนวยความสะดวกสาหรับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน

Technology-neutral

เจ้าของข้อมูลส่วนบุคคล ควรมีความตระหนัก ในการให้ความยินยอม สำหรับการใช้งานข้อมูล ส่วนบุคคล

- แจ้งให้ทราบ
- ความยินยอม

การดำเนินการกับข้อมูล ส่วนบุคคล อยู่ภายใต้ หลักการความยินยอม และวัตถุประสงค์

- การจัดเก็บตาม วัตถุประสงค์
- ข้อจำกัด การเก็บรวบรวม การใช้ การเปิดเผย

Principles-neutral

หน้าที่และภาระผูกพัน ของหน่วยงานในการดูแล ข้อมูลส่วนบุคคล

- ความถูกต้อง
- ข้อจำกัด ในการจัดเก็บ
- ข้อจำกัดในการ โอนย้าย ข้อมูลส่วนบุคคล
- การคุ้มครอง ข้อมูลส่วนบุคคล

ความรับผิดชอบ ของหน่วยงานต่อเจ้าของ ข้อมูลส่วนบุคคล

- การเปิดเผย
- การยอมให้เข้าถึง /แก้ไขข้อมูล
- การปฏิบัติ ตามกฎหมาย

การร้องเรียน

ขอบเขตการบังคับใช้

- ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลฯ ที่เกิดขึ้นในราชอาณาจักร
- ครอบคลุมถึงกรณีผู้ควบคุมและผู้ประมวลผลอยู่นอกราชอาณาจักร หากมีกิจกรรมดังนี้
  - (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่
  - (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร (GDPR Article 3 Territorial scope)

การร้องเรียน

เจ้าของข้อมูล มีสิทธิร้องเรียนในกรณีผู้ควบคุม ผู้ประมวลผลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุม ผู้ประมวลผล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย

ความรับผิดทางแพ่ง

ระบุขอบเขตของการละเมิดข้อมูล เน้นเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติ

- (1) กำหนดความรับผิดของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลเป็นความรับผิดโดยเคร่งครัด (Strict Liability)
- (2) ให้อานาจศาลสั่งให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลชดใช้ค่าสินไหมทดแทนได้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

บทลงโทษอาญา

สาหรับการกระทำที่เป็นความผิดร้ายแรง เช่น การแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสาหรับตนเองหรือผู้อื่น

ม.79 ผู้ควบคุมข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตาม	• ม.27 วรรคหนึ่ง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม) • ม.27 วรรคสอง (ได้รับข้อมูลตามวรรคหนึ่ง เปิดเผยนอกวัตถุประสงค์) • ม.28 (โอนข้อมูลไปต่างประเทศ) เกี่ยวกับข้อมูล ม.26 (Sensitive)โดยทาให้ผู้อื่นเกิดความเสียหาย • ม.27 วรรคสอง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกวัตถุประสงค์ หรือ ส่งหรือโอนข้อมูลส่วนบุคคลที่ Sensitive ไปต่างประเทศ เพื่อแสวงหาผลประโยชน์ที่มิควรได้	ปรับไม่เกิน 5 แสนบาท หรือจำคุกไม่เกิน 6 เดือน ยกเว้นใช้เปิดเผยโดยไม่ได้รับความยินยอมตาม ม.27 วรรคสอง มีโทษปรับไม่เกิน 1 ล้านบาทหรือจำคุกไม่เกิน 1 ปี

บทลงโทษอาญา

สาหรับการกระทำที่เป็นความผิดร้ายแรง เช่น การแสวงหาประโยชน์อันมิควรได้โดยชอบด้วยกฎหมาย สาหรับตนเองหรือผู้อื่น

ม.80 ผู้ใด	• ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตาม พ.ร.บ. นี้ ถ้านำไปเปิดเผยแก่ผู้อื่น	ปรับไม่เกิน 5 แสนบาท หรือจำคุกไม่เกิน 6 เดือน
ม.81นิติบุคคล	• กระทำความผิดตาม พ.ร.บ. นี้ ถ้าการกระทำนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ผู้นั้นต้องรับโทษตามที่บัญญัติไว้ด้วย	

บทลงโทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.82 ผู้ควบคุมข้อมูลไม่ปฏิบัติตาม	• ม.23 ไม่แจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ • ม.30 วรรคสี่ ไม่ปฏิบัติตามเกณฑ์ในการให้เจ้าของเข้าถึงข้อมูล+รับสาเนา • ม.39 วรรคหนึ่งบันทึกรายการให้เจ้าของข้อมูลและสานักงานตรวจสอบ • ม.41 วรรคหนึ่งจัดให้มี DPOหรือ ม.42 วรรคสองสนับสนุน DPO หรือวรรคสาม ไล่ DPO	ปรับไม่เกิน 1 ล้านบาท

บทลงโทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.83 ผู้ควบคุมข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตาม	• ม.21 เก็บ ใช้ รวบรวม เผยแพร่ต้องเป็นไปตามวัตถุประสงค์ • ม.22 เก็บ รวบรวม ให้เท่าที่จาเป็นตามที่กฎหมายกาหนด • ม.24 ข้อยกเว้นการเก็บจากเจ้าของข้อมูลโดยตรง • ม.25 วรรคหนึ่ง (ข้อยกเว้นการเก็บจากแหล่งอื่น) • ม.27 วรรคหนึ่งหรือวรรคสอง (ใช้เปิดเผยโดยไม่มีความยินยอม) • ม.28 โอนไปต่างประเทศ • ม.32 วรรคสอง (สิทธิคัดค้าน ใช้ เปิดเผย) • ม.37 หน้าที่ผู้ควบคุม • ขอความยินยอมโดยการหลอกลวง หรือใช้ผิดวัตถุประสงค์ (ม.21)ซึ่งได้นามาใช้โดยอนุโลมตาม ม.25 วรรคสอง (แจ้งวัตถุประสงค์ใหม่) • ส่งหรือโอนข้อมูล ไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	ปรับไม่เกิน 3 ล้านบาท

บทลงโทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.84 ผู้ควบคุมข้อมูลฝ่าฝืน	• ม.26 Sensitive วรรคหนึ่งหรือวรรคสอง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม) • ม.27 วรรคหนึ่ง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือวรรคสอง นอกเหนือวัตถุประสงค์? • ม.28 ส่งหรือโอนข้อมูลไปต.ป.ท.ซึ่งเป็นข้อมูล ม.26 Sensitive Data • ส่งหรือโอน ที่เป็นข้อมูล ม.26 Sensitive Data โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	ปรับไม่เกิน 5 ล้านบาท
ม.85 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	• ม.41 วรรคหนึ่ง (DPO) หรือ ม.42 วรรคสองหรือวรรคสาม (การไล่ DPO)	ปรับไม่เกิน 1 ล้านบาท
ม.86 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	• ม.40 หน้าที่ผู้ประมวลผล โดยไม่มีเหตุอันควรส่งหรือโอนข้อมูลโดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR) • ม.37(5) ผู้ควบคุมต้องตั้ง DPO ซึ่งได้นามาใช้บังคับโดยอนุโลมตาม ม.38 วรรคสอง (การตั้งตัวแทนในราชอาณาจักร)	ปรับไม่เกิน 3 ล้านบาท

บทลงโทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.87 ผู้ประมวลผลข้อมูล	• ส่งหรือโอนข้อมูลไป ตปท. ตาม ม.26Sensitive Data วรรคหนึ่งหรือวรรคสาม (ประวัติอาชญากรรม) โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	ปรับไม่เกิน 5 ล้านบาท
ม.88 ตัวแทนผู้ควบคุมหรือตัวแทนผู้ประมวลผล	• ไม่ปฏิบัติตาม ม.39 วรรคหนึ่ง (บันทึกรายการ) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.39 วรรคสอง (ตัวแทนผู้ควบคุม) และ ม.41 วรรคหนึ่ง (ตั้ง DPO) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.4 วรรคสี่ (การตั้งตัวแทนในราชอาณาจักร)	ปรับไม่เกิน 1 ล้านบาท
ม.89 ผู้ใด	• ไม่ปฏิบัติตามคาสั่งของคณะกรรมการผู้เชี่ยวชาญตามมาตรา 75หรือไม่ปฏิบัติตาม ม.76 วรรคหนึ่ง (แจ้งให้ส่งหนังสือ) หรือไม่อานวยความสะดวกแก่ พนง.จนท. ตาม ม.76 วรรคสี่	ปรับไม่เกิน 5 แสนบาท

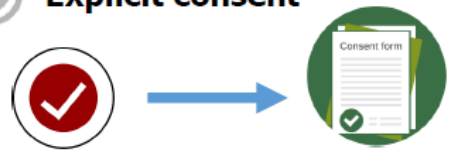
Key changes of the PDPA

Penalties

<= 5,000,000

The PDPA Penalties & fines apply to both Controllers and Processors

Explicit consent

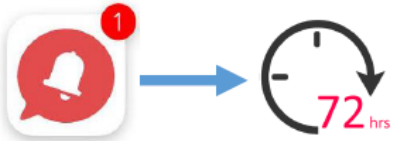


Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Limiting Collection, Use, Disclosure

collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

Breach notification within 72 hours



Reported within 72 hours of first having become aware of the breach.

Right to be forgotten

data subject to have the data controller erase his / her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, in an electronic format (if practicable).

Appointed Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a organisation to demonstrate their compliance to the PDPA

ภาพจาก สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม