กฎหมายคุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ปฏิบัติงานภาครัฐ

(Personal Data Protection Act for Government Officer)

ระหว่างวันที่ ๒๗-๒๘ มกราคม ๒๕๖๘

บุคลากรเข้ารับการฝึกอบรม จำนวน 3 ราย

1. นางสาวจุฬาณี โกวิทยา นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
2. นายชยารพ บุญมัติ นักวิชาการคอมพิวเตอร์ชำนาญการ
3. นางสาวฤทัยชนก สายน้ำทิพย์ นักธรณีวิทยาชำนาญการ

วิทยากร : ผู้ช่วยศาสตราจารย์ ดร.ประพันธ์พงษ์ ขำอ่อน
คณบดีคณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย

CONTENTS

01

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

PDPA

คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
บังคับใช้ ๑ มิถุนายน ๒๕๖๕

<u>มีวัตถุประสงค์</u> ในการคุ้มครองข้อมูลส่วนบุคคล และเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

<u>บังคับใช้กับ</u> ทั้งหน่วยงานภาครัฐ และภาคเอกชน

ย่อมาจาก (Personal Data Protection Act)

ที่มาและเจตนาในการคุ้มครองข้อมูลส่วนบุคคล

สร้างความเชื่อมั่น ให้กับเจ้าของข้อมูลส่วนบุคคลในการเข้ารับบริการ หรือดำเนินกิจกรรมกับหน่วยงานที่ทำการใช้ข้อมูลส่วนบุคคล ว่าหน่วยงานจะมีมาตรการคุ้มครองข้อมูลที่มีมาตรฐาน

ยกระดับการธรรมาภิบาลข้อมูล สร้างหน้าที่ให้กับหน่วยงานทั้งภาครัฐและเอกชนในการสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นปัจจัยสำคัญในการยกระดับการธรรมาภิบาลข้อมูล

ยกระดับสู่มาตรฐานสากล ยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎเกณฑ์และมาตรฐานสากล เพื่อสร้างความเชื่อมั่นให้กับหน่วยงานในต่างประเทศในการดำเนินการค้าและการลงทุนกับประเทศไทย

02

นิยามของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล
Personal Data

นิยาม ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

เช่น ชื่อ นามสกุล เพศ สถานภาพสมรส เลขไอพี เลขหนังสือเดินทาง ฯลฯ

ข้อมูลส่วนบุคคลที่อ่อนไหว

Sentisive Data

ข้อมูลส่วนบุคคลตาม มาตรา 26 ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ และข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

03

ขอบเขตการบังคับใช้ และข้อยกเว้น

ผู้ที่เกี่ยวข้องใน PDPA

เจ้าของข้อมูลส่วนบุคคล
Data Subject

ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

สคส.
PDPC

ผู้ประมวลผลข้อมูลส่วนบุคคล
Data Processor

* สคส. : สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

** PDPC : The Office of the Personal Data Protection Committee

ผู้ควบคุมข้อมูลส่วนบุคคล

Data Controller

หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

รวมถึงหน้าที่ในการรักษาความปลอดภัยข้อมูลให้กับเจ้าของข้อมูล จัดทำบันทึกกิจกรรมการประมวลผลข้อมูลในรูปแบบที่ตรวจสอบได้ แจ้งวัตถุประสงค์ในการเก็บข้อมูล และดำเนินการตามสิทธิของเจ้าของข้อมูล รวมถึงต้องแจ้งเตือนเมื่อเกิดการละเมิดข้อมูลต่อหน่วยงานที่เกี่ยวข้องภายในเวลาที่กำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคล
Data Processor

หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

มีหน้าที่ในการปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล รักษาความมั่นคงปลอดภัยของข้อมูล และจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลต้องไม่เป็นผู้ควบคุมข้อมูลเอง และต้องดำเนินการตามคำสั่งที่ได้รับ ซึ่งหากคำสั่งนั้นขัดต่อกฎหมายจะต้องไม่ปฏิบัติตาม

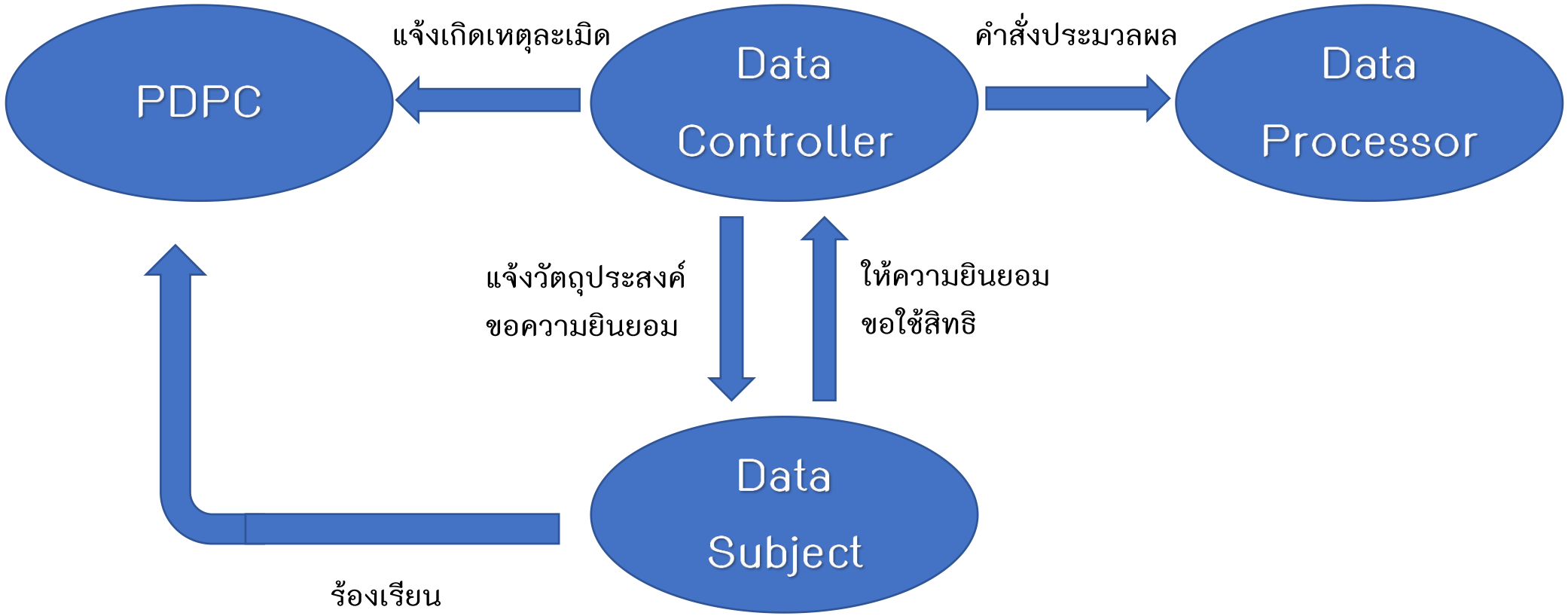
การประมวลผลข้อมูลส่วนบุคคล Personal Data Processing

หมายถึง การดำเนินการ หรือชุดการดำเนินการซึ่งกระทำต่อข้อมูลส่วนบุคคล หรือชุดข้อมูลส่วนบุคคล ด้วยระบบอัตโนมัติหรือไม่ก็ได้

เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การปรับปรุง การใช้ การเปิดเผย การทำให้สามารถเข้าถึงได้ การยับยั้ง หรือการลบหรือทำลายข้อมูลส่วนบุคคล

* ข้อมูลจาก : https://pdpathailand.com/pdpa/content/article9910.php?srsltid=AfmBOooFP6VazQlEFuHhy0QVoTB-sK-fUKO6Ze3qrfjRcKrDLkdc6eEV

03 ขอบเขตการบังคับใช้ และข้อยกเว้น



ไม่ใช้บังคับ

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

ไม่ใช้บังคับ

4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

5. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ทั้งนี้ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน

04

หลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

04 หลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

1. มีความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลและมีความโปร่งใส (Lawful processing and transparency)

2. ใช้ข้อมูลส่วนบุคคล ตามวัตถุประสงค์และเท่าที่จำเป็น (Necessity and Purpose Limitation)

3. ต้องทำข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน (Data Accuracy)

4. มีระยะเวลาในการเก็บข้อมูลส่วนบุคคลที่แน่นอน (Limitation of Storage)

5. มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Security)

6. เคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคลตามขอบเขตที่กฎหมายกำหนด

05

หลักการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

05 หลักการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เก็บ Collection	มีความโปร่งใส (Transparency) ได้แก่ การแจ้งวัตถุประสงค์การเก็บรวบรวมข้อมูลให้กับ Data Subject เก็บเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ (Necessity and Purpose)
ใช้ Usage	ใช้ข้อมูลส่วนบุคคลโดยชอบธรรม (Lawful processing) ใช้เท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้ (Necessity and Purpose) ทำข้อมูลให้มีความถูกต้อง (Data Accuracy)

05 หลักการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เปิดเผย Disclosure	เปิดเผยโดยชอบธรรม (Lawful processing) เปิดเผยเท่าที่จำเป็นและเป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้ (Necessity and Purpose) เปิดเผยอย่างมีความมั่นคงปลอดภัย (Security)
เก็บรักษา Storage / Disposal	เก็บรักษาข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย (Security) กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Limitation of storage)

06

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

1. เป็นธรรมและโปร่งใส

แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) (ม.23)

เพื่อให้เจ้าของข้อมูลส่วนบุคคลทราบว่าการเก็บรวบรวมข้อมูลไปใช้เพื่อวัตถุประสงค์ใด ใช้หรือเปิดเผยอย่างไร และทราบวิธีการติดต่อผู้ควบคุมข้อมูลส่วนบุคคลเพื่อใช้สิทธิหรือสอบถาม ร้องเรียน

มีความชอบธรรมในการประมวลผล (Lawful basis) (ม.24, 26)

ทำการเก็บรวบรวมข้อมูลส่วนบุคคลตามฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

1. ฐานความยินยอม (Consent): เป็นการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2. ฐานสัญญา (Contract): เมื่อมีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญาที่ทำไว้กับเจ้าของข้อมูล

3. ฐานหน้าที่ตามกฎหมาย (Legal Obligation): การประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายที่กำหนดไว้

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

4. ฐานประโยชน์สำคัญต่อชีวิต (Vital Interests): ในกรณีที่มีสถานการณ์ฉุกเฉินและจำเป็นต้องประมวลผลข้อมูลเพื่อป้องกันอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

5. ฐานภารกิจของรัฐ (Public Task): การประมวลผลข้อมูลที่จำเป็นสำหรับภารกิจเพื่อประโยชน์สาธารณะ หรือการปฏิบัติหน้าที่ตามอำนาจรัฐที่ได้รับมอบหมาย

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลแบบทั่วไป (ม.24)

6. ฐานประโยชน์อันชอบธรรม (Legitimate Interests): การประมวลผลข้อมูลเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ส่งผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล

7. ฐานการจัดทำเอกสารประวัติศาสตร์ วิจัย หรือสถิติ (Research/Historical/Statistical): การประมวลผลเพื่อวัตถุประสงค์ดังกล่าว โดยมีเงื่อนไขที่ต้องมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

1. ฐานความยินยอมโดยชัดแจ้ง (Explicit Consent): การที่บุคคลตกลงอย่างเต็มใจและกระทำบางอย่างที่ยืนยันว่าอนุญาตให้องค์กรเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน

2. ฐานการระงับอันตรายต่อชีวิต (Vital Interest): เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

3. ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน (Special Objectives): เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

4. ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Claim of Legal Rights): เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิ เรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

5. ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการแพทย์ ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย และประโยชน์สาธารณะที่สำคัญ (Legal Obligations with Specific Purposes)

ฐานการประมวลผลที่ชอบธรรม (Lawful Basic)

สำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (ม.26)

6. ฐานจำเป็นเพื่อปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์ (Medical Contract)

7. ฐานการเก็บรวบรวมประวัติอาชญากรรมภายใต้การควบคุมของหน่วยงานที่มีอำนาจด้านกฎหมาย

2. จำกัดวัตถุประสงค์และความถูกต้องของข้อมูล

เก็บ ใช้ เปิดเผยเท่าที่จำเป็นและตามวัตถุประสงค์ (ม.22, 27)

การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ห้ามเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ทำข้อมูลส่วนบุคคลให้ถูกต้อง (Data Accuracy) (ม.35)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

3. ความมั่นคงปลอดภัย

จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate Security) (ม.37(1)(2)(4))

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบภายใน 72 ชั่วโมง

4. กำกับดูแลและบริหารจัดการ

ทำบันทึก รายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) (ม.39).

เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

โดยมีข้อมูลอย่างน้อยดังนี้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

4. กำกับดูแลและบริหารจัดการ

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

4. กำกับดูแลและบริหารจัดการ

Data Controller ต้องบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงาน (Records of Processing Activities: RoPA) เพื่อให้เจ้าของข้อมูลส่วนบุคคล หรือ สคส. ตรวจสอบได้ โดยแต่ละกิจกรรมต้องมีการบันทึกรายการข้างต้นเป็นอย่างน้อย

07

การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล DPO

บุคคลที่หน่วยงาน (Data Controller) แต่งตั้งให้ทำหน้าที่กำกับดูแล ควบคุมการดำเนินการ คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้เป็นไปตาม PDPA

<u>หน้าที่</u>

1. ให้คำแนะนำ Data Controller ในการดำเนินการตาม PDPA
2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
3. ประสานงานและให้ความร่วมมือกับ สำนักงานฯ
4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมาย

** PDPA อนุญาตให้ DPO เป็นได้ทั้งคนในหน่วยงานหรือ Outsource

08

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

Data Controller ต้องดำเนินการเมื่อเกิดเหตุละเมิด

1. เมื่อทราบถึงเหตุละเมิดข้อมูลส่วนบุคคล ต้องแจ้ง สคส. ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

2. ในกรณีที่การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (High Risk) ให้แจ้งเหตุละเมิดนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า

3. กำหนดใน PDPA ให้ Data Processor แจ้งเหตุ Data Breach ให้ Data Controller ทราบ โดยไม่ชักช้า ภายใน 72 ชม.

Data Processor ต้องดำเนินการเมื่อเกิดเหตุละเมิด

แจ้ง ให้ Data Controller ทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ที่ทราบเหตุ

09

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

1. เก็บ ใช้ เปิดเผยตามคำสั่ง ของ Data Controller

2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

3. แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ Data Controller ทราบภายใน 72 ชั่วโมง

4. ทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) (ม.39)*

5. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)*

10

การโอนข้อมูลส่วนบุคคลข้ามพรมแดน

การโอนข้อมูลข้ามพรมแดน (ม.28)

ประเทศผู้รับข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามที่ สคส. กำหนด (Adequacy) หรือเข้าข้อยกเว้นที่ทำให้โอนข้อมูลไปได้

11

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิในการเพิกถอนความยินยอมที่เคยให้ไว้เมื่อใดก็ได้ (ม.19)

2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล (Right of access) (ม.30)

3. สิทธิในการขอให้โอนข้อมูลส่วนบุคคลไปยัง Data Controller อื่นด้วยวิธีการอัตโนมัติ (Right of portability) (ม.31)

4. สิทธิขอคัดค้าน การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล (Right to Object) (ม.32)

5. สิทธิขอให้ลบทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure) (ม.33)

6. สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict) (ม.34)

7. สิทธิในการขอแก้ไขให้ข้อมูลส่วนบุคคลมีความถูกต้อง (Right to Rectification) (ม.35)

12

บทลงโทษตามกฎหมาย

การปรับทางปกครอง (ม.82-90) (1-5 ล้านบาท)

คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม.90)

ความรับผิดทางแพ่ง (ม.77-78)

เมื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรม เท่านั้น ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริงแต่ไม่เกินสองเท่าของค่าสินไหมทดแทนแท้จริง

ทางอาญา (ม.79-81) โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท

(เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดเรื่อง

(1) แสวงหาผลประโยชน์จากข้อมูลส่วนบุคคลที่อ่อนโหว หรือ

(2) ทำให้เกิดการเสียชื่อเสียง การดูหมิ่น เกลียดชัง หรือได้รับความอับอายจากการใช้ข้อมูลส่วนบุคคลที่อ่อนโหว

มาตรการที่ สคส. จะนำมาพิจารณาโทษปรับปกครอง จะดูจากพฤติกรรมของหน่วยงาน (ม.8 ประกาศฯ เรื่องแนวทางพิจารณาโทษปรับปกครอง) ในด้านต่อไปนี้

- เจตนาหรือความจงใจในการกระทำผิด
- ความระมัดระวัง
- มูลค่าความเสียหายและความร้ายแรงของเหตุ
- ระดับความรับผิดชอบและมาตรฐานด้าน PDPA ขณะที่เหตุเกิด
- การดำเนินการตามแนวปฏิบัติทางธุรกิจ หรือมาตรฐานด้านความมั่นคงปลอดภัย
- การเยียวยาและบรรเทาเหตุขณะที่เหตุเกิดขึ้น

Thank YOU