PDPA

พันตำรวจเอก ดร.สีหนาท ประยูรรัตน์

ที่ปรึกษาอาวุโส Inter Consultants Law&Business Ltd.

www.Seehanat.com

Timeline การบังคับใช้กฎหมาย

1 มิถุนายน 2565

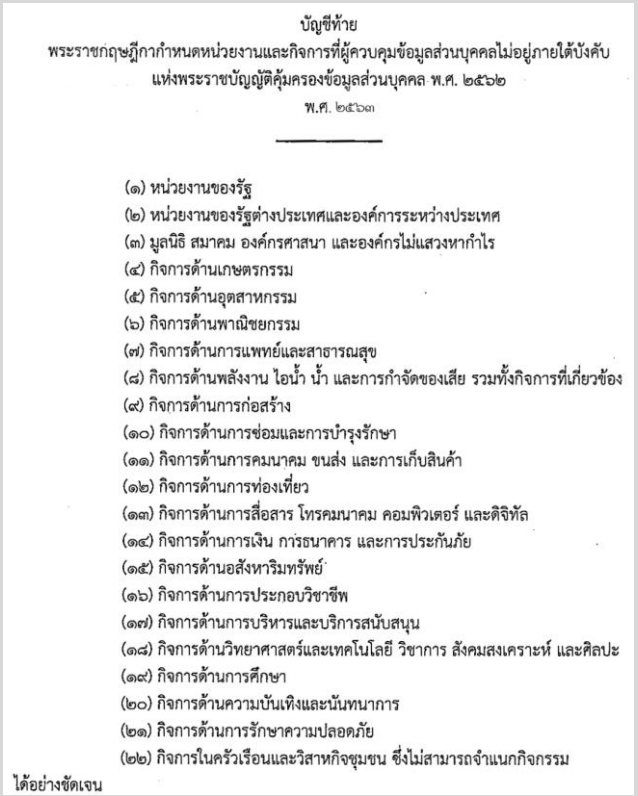
มีผลบังคับใช้

27 พฤษภาคม 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

21 พฤษภาคม 2563

พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 และ ฉบับที่ 2 พ.ศ. 2564



บัญชีท้าย
พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
พ.ศ. ๒๕๖๓

(๑) หน่วยงานของรัฐ
(๒) หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ
(๓) มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร
(๔) กิจการด้านเกษตรกรรม
(๕) กิจการด้านอุตสาหกรรม
(๖) กิจการด้านพาณิชยกรรม
(๗) กิจการด้านการแพทย์และสาธารณสุข
(๘) กิจการด้านพลังงาน ไอน้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง
(๙) กิจการด้านการก่อสร้าง
(๑๐) กิจการด้านการซ่อมและการบำรุงรักษา
(๑๑) กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า
(๑๒) กิจการด้านการท่องเที่ยว
(๑๓) กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล
(๑๔) กิจการด้านการเงิน การธนาคาร และการประกันภัย
(๑๕) กิจการด้านอสังหาริมทรัพย์
(๑๖) กิจการด้านการประกอบวิชาชีพ
(๑๗) กิจการด้านการบริหารและบริการสนับสนุน
(๑๘) กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ
(๑๙) กิจการด้านการศึกษา
(๒๐) กิจการด้านความบันเทิงและนันทนาการ
(๒๑) กิจการด้านการรักษาความปลอดภัย
(๒๒) กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรม
ได้อย่างชัดเจน

ข้อมูลส่วนบุคคลที่เก็บ รวบรวม ใช้ ก่อนที่กฎหมายจะมีผลบังคับใช้

ข้อมูลส่วนบุคคลที่เคยเก็บไว้

1 มิถุนายน 2564

จัดให้มีวิธีการยกเลิกความยินยอมให้เก็บ ใช้ เปิดเผย ข้อมูลเหล่านี้

เผยแพร่/ประชาสัมพันธ์ ให้เจ้าของข้อมูลแจ้งยกเลิกการเก็บ ใช้ ข้อมูลของตนได้โดยง่าย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

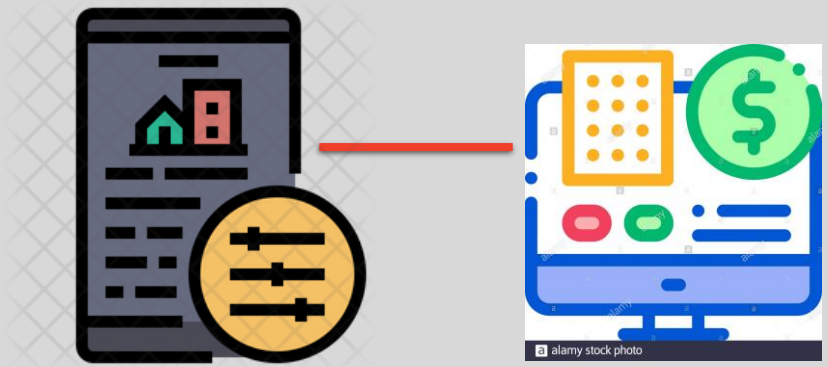
Concept

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เจ้าของข้อมูลส่วนบุคคล
(Data Subject)

มีส่วนร่วมในการบริหารจัดการข้อมูลของตนเอง ที่ผู้อื่นเก็บ รวบรวม ใช้ เปิดเผย

Liability (ความรับผิดตามกฎหมาย)



ผู้ควบคุมข้อมูล
Data Controller

ผู้ประมวลผลข้อมูล
Data Processor

มีผลบังคับใช้
1 มิถุนายน 2564

เหตุผล/เจตนารมณ์ของกฎหมาย

ซื้อผลิตภัณฑ์/บริการ
การลงทุน/การกู้ยืมเงิน

ธุรกรรมทางการเงิน
กิจกรรมทางธุรกิจ

องค์กรธุรกิจ/สหกรณ์/นิติบุคคลต่างๆ

ผู้ประมวลผลข้อมูลต่างๆ

ตัวแทนขาย/คู่ค้า

ยักยอกขายข้อมูล

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

Cambridge Analytica

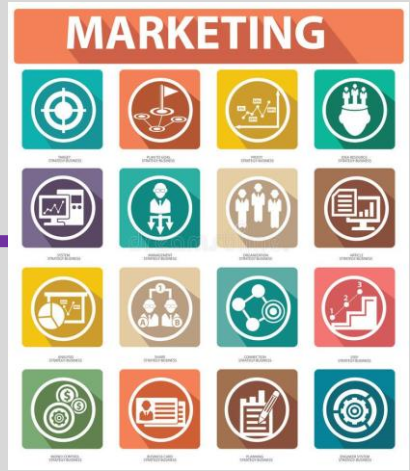
นำข้อมูลส่วนบุคคลของผู้ใช้ (กว่า 50 ล้านคน) ไปวิจัย/ประมวลผลด้านความเห็นทางการเมือง เพื่อประโยชน์ในแคมเปญหาเสียงเลือกตั้งในสหรัฐอเมริกา

รายได้ของเฟสบุ๊ค 55,000 ล้านเหรียญสหรัฐ (2018)

The Federal Trade Commission : FTC ปรับกรณีละเมิดข้อมูลส่วนบุคคล ประมาณ 5,000 กว่าล้านเหรียญสหรัฐ คิดเป็นประมาณ 10% ของรายได้ในปีนั้น

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

Google™



ประมวลผล/วิเคราะห์ข้อมูลผู้เยาว์ เพื่อขายโฆษณาแบบเจาะจง (Re-target Ad) โดยไม่ขอความยินยอมจากผู้ปกครอง รวมถึงการขอ Consent แบบแอบซ่อนในขั้นตอนการสมัคร Google Account และนำข้อมูลสมาชิกไปทำ Personalized Ad

รายได้ของ **Google** ประมาณ **130,000** ล้านเหรียญสหรัฐ (**2018**)

The Federal Trade Commission : FTC ปรับกรณีละเมิดข้อมูลส่วนบุคคล ประมาณ **300** กว่าล้านเหรียญสหรัฐ คิดเป็นประมาณ **1.5%** ของรายได้ในปีนั้น

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

ข้อมูลการจองตั๋วเครื่องบินและการชำระเงิน

HACK

BRITISH AIRWAYS

รายได้ของ **British Airways** ประมาณ 13,000 ล้านปอนด์ (2018)

UK Information Commissioner's Office : ICO ปรับกรณีถูกเจาะข้อมูลส่วนบุคคลประมาณ 500,000 คน ค่าปรับ 204 ล้านปอนด์ คิดเป็นประมาณ 1% ของรายได้ในปีนั้น

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

Marriott INTERNATIONAL

ข้อมูลรายละเอียดบัตรเครดิต หนังสือเดินทาง ข้อมูลการชำระเงินของลูกค้าประมาณ **339** ล้านคน ถูกเจาะระบบและขโมยข้อมูล

ถูกปรับตามกฎหมาย **GDPR** (สหภาพยุโรป) **99.2** ล้านปอนด์

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

SingHealth
Defining Tomorrow's Medicine

HACK

ข้อมูลชื่อ/ที่อยู่ ของผู้ป่วยกว่า 1.5 ล้านราย ถูกเจาะระบบและขโมยข้อมูล รวมถึงข้อมูลการจ่ายยาให้กับผู้ป่วยประมาณ 160,000 รายก็ได้ถูกโจรกรรมไปด้วย (ข้อมูลของนายกรัฐมนตรี Lee Hsien Loong ก็เป็นหนึ่งในนั้นด้วย)

The Personal Data Protection Commission (PDPC) ปรับ 1 ล้านเหรียญสิงคโปร์

หมายเหตุ : PDPC มีการปรับนิติบุคคลกว่า 100 องค์กร (ทั้งภาคอุตสาหกรรม การค้า การเงิน วิชาชีพเฉพาะทาง รวมถึงองค์กรการกุศล ที่มีระบบการป้องกันรักษาความปลอดภัยข้อมูลที่ไม่ตรงตามมาตรฐาน ในปี 2019 มียอดปรับ 1.54 ล้านเหรียญสิงคโปร์

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในประเทศ

PR2021_35

บางกอกแอร์เวย์ส ชี้แจงกรณีตรวจสอบพบความผิดปกติในระบบเครือข่ายของบริษัทฯ

กรุงเทพฯ / 26 สิงหาคม 2564 – เมื่อวันที่ 23 สิงหาคม 2564 บริษัท การบินกรุงเทพ จำกัด (มหาชน) หรือสายการบินบางกอกแอร์เวย์ส ถูกโจมตีด้านความปลอดภัยทางไซเบอร์ ซึ่งส่งผลให้มีการเข้าถึงระบบสารสนเทศของบริษัทฯ โดยไม่ชอบด้วยกฎหมายและโดยไม่ได้รับอนุญาต

เมื่อบริษัทฯ ทราบเหตุการณ์ดังกล่าว บริษัทฯ ร่วมกันกับผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้ดำเนินการตรวจสอบ และควบคุมเหตุการณ์ที่เกิดขึ้นโดยทันที ในขณะนี้ บริษัทฯ อยู่ระหว่างดำเนินการสืบสวนอย่างเร่งด่วนเพื่อระบุข้อมูลอาจได้รับความเสียหาย และผู้โดยสารที่ได้รับผลกระทบ รวมถึงดำเนินมาตรการที่เกี่ยวข้องเพื่อปรับปรุงระบบ สารสนเทศของบริษัทฯ ให้มีความเข้มแข็งมากยิ่งขึ้น

จากการตรวจสอบเบื้องต้น บริษัทฯ พบว่าอาจมีข้อมูลส่วนบุคคลที่ถูกเข้าถึงโดยไม่ชอบด้วยกฎหมาย และไม่ได้รับอนุญาต อาทิ ชื่อ นามสกุล สัญชาติ เพศ หมายเลขโทรศัพท์ อีเมล ที่อยู่ ช่องทางการติดต่อสื่อสาร ข้อมูลหนังสือเดินทาง ประวัติการเดินทาง ข้อมูลบัตรเครดิตบางส่วน และข้อมูลอาหารพิเศษของผู้โดยสาร อย่างไรก็ตาม บริษัทฯ ขอยืนยันว่าเหตุการณ์ที่เกิดขึ้นดังกล่าวไม่มีผลกระทบต่อการดำเนินธุรกิจของบริษัทฯ และระบบความปลอดภัยด้านการบิน

บริษัทฯ ได้รายงานเหตุการณ์ดังกล่าวไปยังสำนักงานตำรวจแห่งชาติและหน่วยงานที่เกี่ยวข้องแล้ว และเพื่อเป็นการป้องกันในเบื้องต้น บริษัทฯ แนะนำให้ผู้โดยสารติดต่อไปยังธนาคาร หรือผู้ให้บริการบัตรเครดิต และดำเนินการตามคำแนะนำของหน่วยงานดังกล่าว และเปลี่ยนรหัสผ่านที่อาจได้รับผลกระทบโดยเร็วที่สุด

นอกจากนี้บริษัทฯ ขอให้ระมัดระวังกลโกงทางโทรศัพท์ รวมถึงอีเมลที่น่าสงสัยและมิชอบ เนื่องจากผู้โจมตีระบบอาจอ้างตนว่าเป็นสายการบินบางกอกแอร์เวย์ส เพื่อพยายามหลอกลวงในการรวบรวมข้อมูลส่วนบุคคล (หรือที่เรียกกันว่า "phishing") ทั้งนี้ บริษัทฯ ไม่มีนโยบายที่จะติดต่อผู้โดยสารเพื่อขอข้อมูลเกี่ยวกับบัตรเครดิต และ/หรือ ข้อมูลทางการเงิน และหากเกิดเหตุการณ์ดังกล่าวผู้โดยสารควรดำเนินการตามกฎหมาย

สำหรับผู้โดยสารที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว สามารถติดต่อสายการบินฯได้ตามช่องทางต่าง ๆดังนี้
- ภายในประเทศ หมายเลขโทรศัพท์ 1800-010-171 (ไม่เสียค่าบริการ) เวลา 08.00 น. – 17.30 น.
- ต่างประเทศ หมายเลขโทรศัพท์ 800-8100-6688 เวลา 08.00 น. – 17.30 น.(ตามเวลาประเทศไทย)
- อีเมล infosecurity@bangkokair.com

บริษัทฯ ให้ความสำคัญในการปกป้องและเก็บรักษาข้อมูลส่วนบุคคลของผู้โดยสารเป็นสิ่งสำคัญสูงสุด และบริษัทฯ ขออภัยต่อความกังวล และความไม่สะดวกที่เกิดขึ้นจากเหตุการณ์ในครั้งนี้

****

ข้อมูลเพิ่มเติมกรุณาติดต่อ
แผนกสื่อมวลชนสัมพันธ์
สายการบินบางกอกแอร์เวย์ส
E-mail: media@bangkokair.com

ตัวอย่างการละเมิดข้อมูลส่วนบุคคลในประเทศ

หลุดจริง! “ทปอ.” รับข้อมูลผู้สอบ TCAS64 ถูกแฮกขาย 23,000 รายการ

หลุดจริง! “ทปอ.” ยอมรับข้อมูลผู้สมัครสอบ TCAS64 ถูกแฮกเอาไปประกาศขาย 23,000 รายการ เร่งตรวจสอบระบบ-รวบรวมหลักฐานส่งเจ้าหน้าตำรวจ ฟากโซเชี่ยลติดแฮชแท็ก “แบนทปอ”

03/02/2022

ทปอ
สมาคมที่ประชุมอธิการบดีแห่งประเทศไทย
Association of The Council of University Presidents of Thailand

ประกาศที่ประชุมอธิการบดีแห่งประเทศไทย
เหตุภัยคุกคามทางไซเบอร์ระบบการคัดเลือกกลางบุคคลเข้าศึกษาต่อในสถาบันอุดมศึกษา (TCAS)

ด้วยวันที่ 1 ก.พ. 2565 ปรากฏข้อมูลข่าวสารการประกาศจำหน่ายข้อมูลในอินเตอร์เน็ตจำนวน 23,000 รายการ ถูกกล่าวอ้างว่า เป็นข้อมูลส่วนบุคคลของระบบการคัดเลือกกลางบุคคลเข้าศึกษาในสถาบันอุดมศึกษา (TCAS) จากเว็บไซต์ mytcas.com ทั้งนี้ ได้มีการแสดงข้อมูลตัวอย่าง เช่น ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน ผลคะแนนตามเกณฑ์การคัดเลือกของสาขาวิชาที่สมัคร เป็นต้น ขณะนี้ ทาง ทปอ. ได้ตรวจสอบทั้งหมดในไฟล์ตัวอย่างแล้ว พบว่า เป็นข้อมูลของระบบ TCAS64 ในรอบที่ 3 ซึ่งไม่ใช่ข้อมูลส่วนบุคคลทั้งหมดของผู้สมัคร และเป็นข้อมูลในรูปแบบ CSV ที่เจ้าหน้าที่ที่ได้รับมอบหมายของแต่ละสถาบันอุดมศึกษาดึงออกจากระบบเพื่อประมวลผลคัดเลือกของแต่ละสาขาวิชาที่เปิดรับในสถาบันฯ โดยเจ้าหน้าที่สามารถเข้าถึงได้เฉพาะข้อมูลผู้สมัครในรอบ 3 ของสถาบันนั้น ๆ ซึ่งข้อมูลในรอบ 3 ของระบบ TCAS64 มีทั้งหมด 826,250 รายการ แต่ที่ผู้ขายข้อมูลกล่าวอ้างนั้น มีเพียง 23,000 รายการ โดยคาดว่าเป็นไฟล์ที่สร้างขึ้นในช่วงเดือนพฤษภาคม 2564 ที่เจ้าหน้าที่ของสถาบันอุดมศึกษาดึงข้อมูลคะแนนไปจัดเรียงลำดับผู้สมัคร(Ranking) ตามเกณฑ์คัดเลือกของแต่ละสาขาวิชา ซึ่งข้อมูลที่นำเสนอขายไม่มีผลการจัดเรียงลำดับ Ranking ของผู้สมัคร

ปัจจุบัน ทปอ. ได้ปิดระบบ TCAS64 ไปแล้วตั้งแต่เดือนธันวาคม 2564 และ สำหรับระบบ TCAS65 มีการเปลี่ยนระบบเป็นรูปแบบใหม่ และเว็บไซต์ที่พัฒนาขึ้นใหม่ในปีนี้ มีการจัดเก็บไฟล์ข้อมูลที่มีความอ่อนไหวในรูปแบบ Private ที่ไม่สามารถเข้าถึงโดยตรงได้ การที่จะเข้าถึงไฟล์ข้อมูลได้นั้น ผู้ใช้งานระบบต้องได้รับการอนุญาตจากระบบ (presigned URL) ที่มีอายุในเวลาที่กำหนดเท่านั้น ซึ่งผู้ใช้งานระบบสามารถเข้าถึงข้อมูลได้ชั่วคราว พร้อมระบบบันทึกการใช้งานอย่างละเอียด

อย่างไรก็ตาม ทปอ. ขออภัยอย่างสูงสำหรับผลกระทบที่เกิดขึ้นกับข้อมูลส่วนบุคคลที่ถูกกล่าวอ้าง ตลอดจนตระหนักถึงการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์ จากเหตุการณ์ดังกล่าว จึงได้มีการตรวจสอบระบบและกระบวนการทำงานอย่างละเอียด ซึ่งได้รับการสนับสนุนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และอยู่ระหว่างการรวบรวมพยานหลักฐานที่เกี่ยวข้องเพื่อดำเนินการแจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ และแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อรับทราบสถานการณ์ต่อไป

ทปอ. ขอยืนยันว่า ระบบ TCAS65 มีความปลอดภัยในการใช้งาน และ มีการเฝ้าระวังสิ่งผิดปกติ ร่วมกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) อย่างใกล้ชิด เพื่อให้คงไว้ซึ่งความน่าเชื่อถือในระบบและกระบวนการคัดเลือกต่อไป

ประกาศ ณ วันที่ 2 กุมภาพันธ์ 2565

บทลงโทษ

ต่างประเทศ

สหภาพยุโรป

สูงสุดไม่เกิน **20** ล้านยูโร หรือ **4** เท่าของรายได้ทั้งปี

สิงคโปร์

สูงสุดไม่เกิน **1** ล้านเหรียญสิงคโปร์

มาเลเซีย

สูงสุดไม่เกิน **5** แสนริงกิต

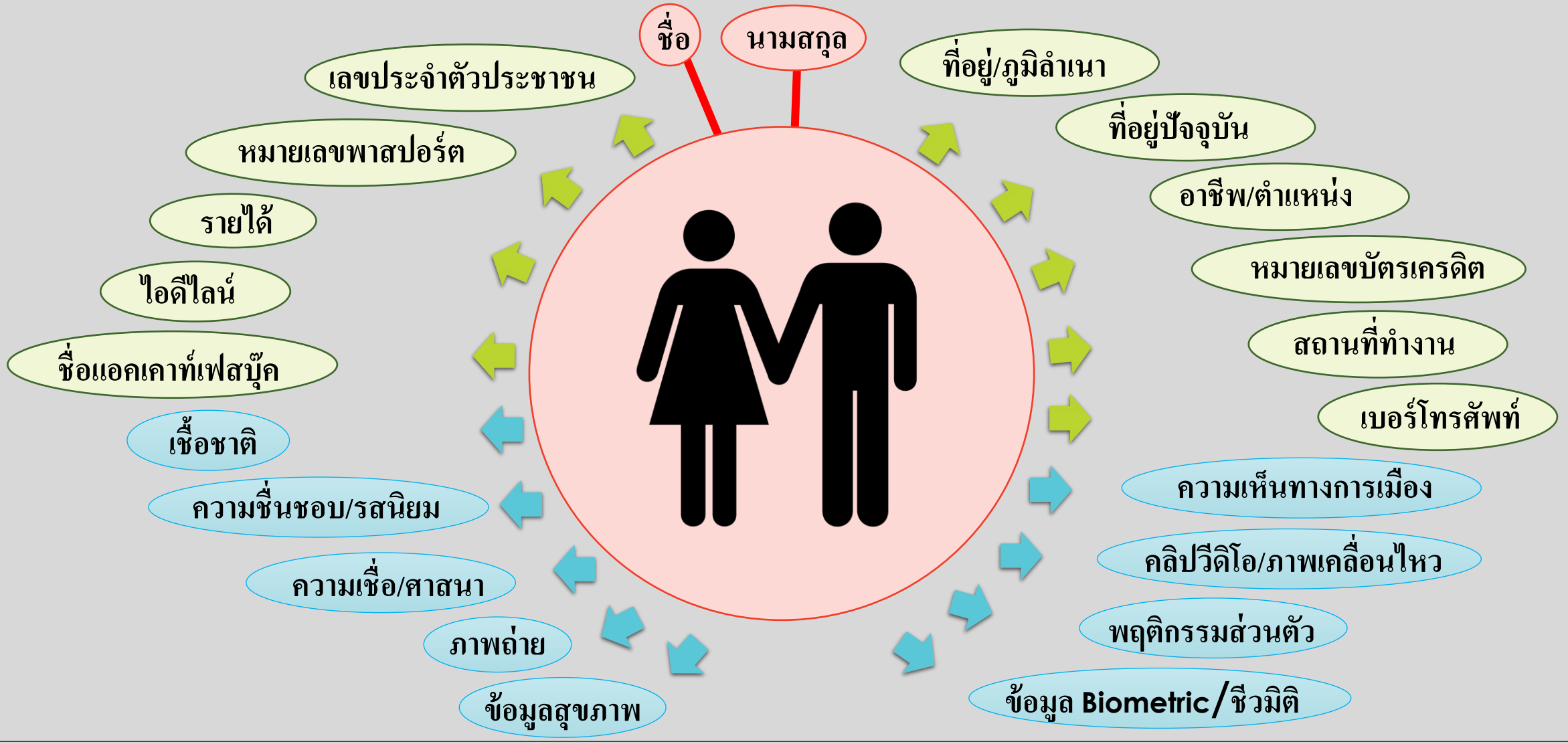
ประเทศไทย

มาตรการลงโทษ	อัตราโทษ
มาตรการทางแพ่ง	ค่าเสียหายตามจริง และ ค่าสินไหมทดแทน **สูงสุด 2 เท่า**ของค่าเสียหายตามจริง
มาตรการทางอาญา	โทษจำคุกสูงสุด **1 ปี** ปรับไม่เกิน **1,000,000** บาท หรือ ทั้งจำทั้งปรับ
มาตรการทางปกครอง	โทษปรับตั้งแต่ **1,000,000 – 5,000,000** บาท
หมายเหตุ : หากผู้กระทำผิดเป็น**นิติบุคคล** กรรมการ ผู้จัดการ ผู้สั่งการ บุคคลผู้รับผิดชอบในการดำเนินการ ต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81)	

ข้อยกเว้น ที่ไม่ใช้บังคับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (ไม่ได้รับการคุ้มครองหรือไม่ต้องปฏิบัติตามกฎหมายนี้)

- การเก็บ/การใช้/การเปิดเผย ข้อมูลส่วนบุคคลที่ทำขึ้นเพื่อประโยชน์ส่วนตัว/กิจกรรมในครอบครัวของตน
- การดำเนินการของหน่วยงานรัฐที่มีหน้าที่รักษาความมั่นคง (ความมั่นคงทางการคลัง การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ ความมั่นคงปลอดภัยทางไซเบอร์)
- บุคคล/นิติบุคคล ซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน ศิลปกรรม วรรณกรรมตามจริยธรรมของวิชาชีพหรือประโยชน์สาธารณะเท่านั้น
- สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมาธิการที่รัฐสภาแต่งตั้ง โดยใช้ข้อมูลส่วนบุคคลภายใต้อำนาจหน้าที่เท่านั้น
- การพิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนพิจารณาคดี บังคับคดี วางทรัพย์ และกระบวนการยุติธรรมทางอาญา
- การดำเนินการกับข้อมูลของเครดิตบูโรและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ข้อมูลส่วนบุคคล คืออะไร : Personal Data & Sensitive Data



ท่านเป็น “องค์ประกอบใด” ของการคุ้มครองข้อมูลส่วนบุคคล

ถ้าท่านเป็น **“ผู้ที่ได้รับข้อมูลส่วนบุคคล หรือ เป็นผู้ขอข้อมูลส่วนบุคคลจากเจ้าของข้อมูล(ลูกค้าบุคคลธรรมดา)”** ไม่ว่าท่านจะ เก็บรวบรวม ใช้ เปิดเผย ในทางธุรกิจ หรือประโยชน์อื่นใด หรือนำมาส่งต่อไปยังบุคคลอื่นๆเพื่อดำเนินการใดๆทางธุรกิจ

→ **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)**

ถ้าท่านเป็น “ ผู้ที่ปฏิบัติตามที่ได้รับมอบหมาย ในการรับข้อมูลส่วนบุคคล มาจากองค์กร/บริษัทอื่น ซึ่งบริษัทดังกล่าวเป็นผู้ได้รับข้อมูลส่วนบุคคลหรือขอข้อมูลส่วนบุคคลมาจากเจ้าของข้อมูล(ลูกค้าบุคคลธรรมดา)” โดยท่านมีหน้าที่นำข้อมูลส่วนบุคคลนั้น มาใช้วิเคราะห์ หรือ ดำเนินการใดๆอันเป็นการใช้หรือบริหารข้อมูลตามข้อตกลงหรือคำสั่งของบริษัทที่ส่งข้อมูลมาให้ท่าน

→ **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** ***(ต้องไม่ใช่ผู้ควบคุมข้อมูล)***

ถ้าท่านเป็น “ผู้ให้ข้อมูล**ของตนเอง** กับผู้อื่น ไม่ว่าจะด้วยวัตถุประสงค์ทางธุรกิจ การใช้บริการ ข้อตกลงอื่นๆ

→ **เจ้าของข้อมูลส่วนบุคคล (Data Subject)**

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

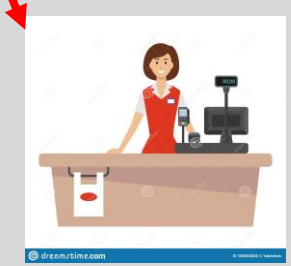
บจก. กฎหมายและธุรกิจ อินเตอร์ คอนซัลแตนท์
Inter Consultants Law & Business Ltd.

Company/Business

SERVICES

PRODUCTS

INVESTMENT : หลักทรัพย์/กองทุนรวม/สหกรณ์



Customers/Members/Users

Personal Data

บทบาทของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

เก็บ รวบรวม ใช้ เปิดเผย

วัตถุประสงค์ที่จำเป็น
- ลงทะเบียนสมาชิก
- ทำสัญญา
- ดำเนินการเพื่อสนับสนุนการขาย
- ดำเนินการเพื่อส่งเสริมการให้บริการ
- ปฏิบัติตามกฎหมายที่เกี่ยวข้อง

ขอความยินยอม (Consent)

- ชัดแจ้ง
- เข้าใจง่าย
- ช่องทางสะดวก
- อิสระในการยินยอม
- ระบุวัตถุประสงค์ชัดเจน

ช่องทางในการใช้สิทธิ

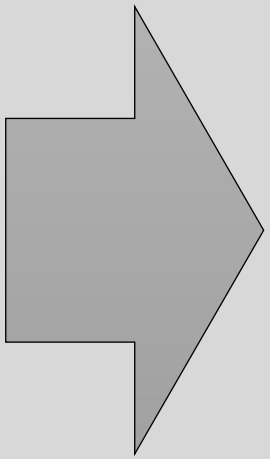
ขอเพิกถอนความยินยอม
- สิทธิในการเข้าถึงและขอสำเนาข้อมูล
- สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล
- สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน
- สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล
- สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล
- สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน

รักษาความมั่นคงปลอดภัยของข้อมูล

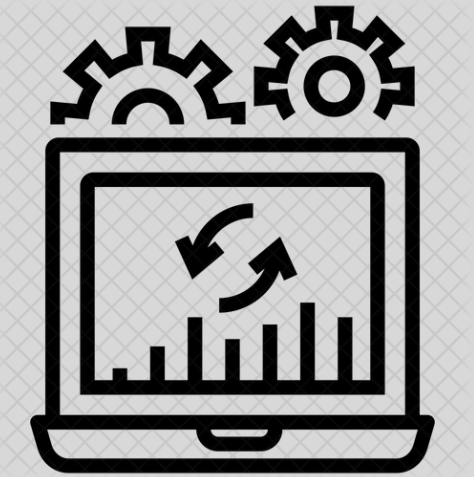
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ข้อมูลส่วนบุคคลของสมาชิก/ลูกค้า



ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)



หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล : การขอความยินยอม (Consent)

- ผู้ควบคุมข้อมูลฯ มีหน้าที่ต้อง **ขอความยินยอม ก่อน หรือ ขณะ เก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล**จากเจ้าของข้อมูลฯ
- ผู้ควบคุมข้อมูลจะต้องเก็บข้อมูลส่วนบุคคล**เท่าที่จำเป็น**จะต้องใช้ตามวัตถุประสงค์ที่มีเท่านั้น

รูปแบบการขอความยินยอม

- ต้องขอโดย**ชัดแจ้ง** ด้วยวิธี**เป็นหนังสือ**หรือผ่าน**ระบบอิเล็กทรอนิกส์** (เว้นแต่โดยสภาพไม่อาจขอด้วยวิธีดังกล่าวได้)
- แจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลฯ
- การขอความยินยอม ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
- มีวิธีการที่เข้าถึงได้ง่าย
- ถ้อยคำและภาษาที่ใช้ต้องเข้าใจได้ง่าย ไม่ทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ของการขอความยินยอม
- การขอความยินยอม ต้องคำนึงถึง “อิสระของเจ้าของข้อมูลในการให้ความยินยอม”
- (โดยต้องไม่มีเงื่อนไขบังคับให้ต้องยินยอม เพื่อเข้าถึงบริการหรือทำสัญญา)

รูปแบบการขอความยินยอม : Consent Form

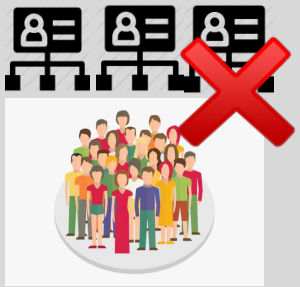
ชัดแจ้ง (แยกออกจากส่วนอื่นๆของสัญญาหรือข้อชี้แจงต่างๆ)

มีช่องทางให้ยินยอมได้สอดคล้องกับการเก็บข้อมูล และไม่บังคับให้ต้องยินยอม

แจ้งวัตถุประสงค์ในการเก็บ รวบรวม ใช้ และระยะเวลาในการเก็บข้อมูล

ผลของการขอความยินยอมที่ไม่ถูกต้องตามกฎหมาย

ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูล เก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลไม่ได้

เหตุยกเว้น การขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 24)

(1) Research : วัตถุประสงค์ในการจัดทำ**เอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ** หรือที่เกี่ยวกับการ**ศึกษาวิจัยหรือสถิติ**ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) Vital Interest : เพื่อ**ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ**ของบุคคล

(3) Contract : เป็นการจำเป็นเพื่อการ**ปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา**หรือ เพื่อใช้ในการดำเนินการตามคำขอของ เจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (เป็นฐานยกเว้นความยินยอมของภาคธุรกิจมากที่สุด)

(4) Public Task : เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจ**เพื่อประโยชน์สาธารณะ**ของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการ**ใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูล**ส่วนบุคคล เช่น ธุรกิจที่รับมอบหมายจากหน่วยงานรัฐโดยตรง

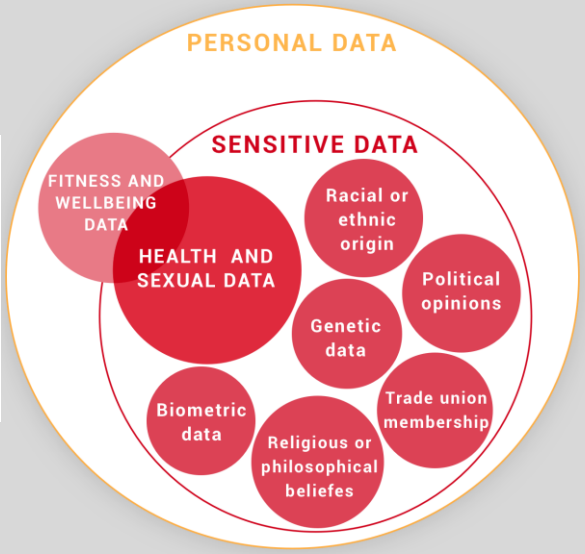
(5) Legitimate Interest : เป็นการจำเป็น**เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล** หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าว<u>มีความสำคัญ น้อยกว่าสิทธิขั้นพื้นฐาน</u>ในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) Legal Obligation : เป็นการ**ปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล**

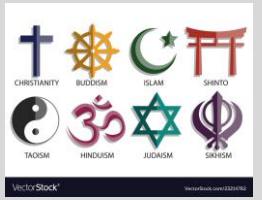
บจก. กฎหมายและธุรกิจ อินเตอร์ คอนซัลแตนท์
Inter Consultants Law & Business Ltd.

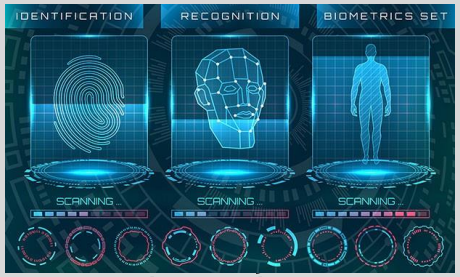
ข้อมูล(ส่วนบุคคล)ที่อ่อนไหว **Sensitive Data**

มาตรา 26 กำหนด “ข้อมูลอ่อนไหว”



- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ/ชีวมิติ
- ข้อมูลอื่นๆที่กระทบต่อเจ้าของข้อมูลในทำนองเดียวกันนี้ (คณะกรรมการประกาศกำหนด)





ต้องได้รับความยินยอมโดยชัดแจ้ง

ข้อยกเว้น ไม่ต้องขอความยินยอมในการเก็บข้อมูลอ่อนไหว Sensitive Data

ผู้ควบคุมข้อมูลส่วนบุคคล อาจไม่ต้องขอความยินยอม ถ้าการเก็บรวบรวมข้อมูลนั้น ดำเนินการเพื่อ

1. เพื่อป้องกัน ระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของบุคคล ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้
2. เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมาย (ที่มีความคุ้มครองที่เหมาะสม) ของมูลนิธิ สมาคม สหภาพแรงงาน องค์กรที่ไม่แสวงหาผลกำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา ให้แก่สมาชิก/ผู้เคยเป็นสมาชิก/ผู้ที่ติดต่ออย่างสม่ำเสมอ โดยไม่มีการเปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกองค์กร
3. ข้อมูลนั้นเป็นข้อมูลที่เปิดเผยต่อสาธารณะภายใต้การยินยอมโดยชัดแจ้งของเจ้าของข้อมูล
4. เป็นการจำเป็น เพื่อให้เกิดสิทธิเรียกร้องตามกฎหมาย หรือเป็นการปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย หรือยกขึ้นเพื่อต่อสู้สิทธิเรียกร้อง
5. เป็นการจำเป็น เพื่อปฏิบัติตามกฎหมาย ในวัตถุประสงค์เกี่ยวกับ
   - การแพทย์และสุขภาพ
   - สาธารณสุขของสาธารณะ การคุ้มครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการรักษาพยาบาลของผู้มีสิทธิ การคุ้มครองผู้ประสบภัยจากรถ
   - การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติหรือประโยชน์สาธารณะอื่น
   - ประโยชน์สาธารณะที่สำคัญ

หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล : การขอถอนความยินยอม

<u>การขอถอนความยินยอม</u> (เมื่อเจ้าของข้อมูลฯได้เคยให้ความยินยอมไว้ เจ้าของข้อมูลฯ ประสงค์จะเพิกถอนการยินยอมให้ใช้หรือเปิดเผยข้อมูลได้)

- เจ้าของข้อมูล จะเพิกถอน/ยกเลิก การให้ความยินยอมในการใช้/เปิดเผยข้อมูล **เมื่อใดก็ได้** เว้นแต่มีข้อจำกัดสิทธิห้ามเพิกถอนตามกฎหมายหรือตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลฯ)

- การเพิกถอน จะต้อง**ง่าย/สะดวก** เสมือนขั้นตอนในการให้ความยินยอม

- การเพิกถอนการยินยอม ไม่กระทบต่อการเก็บ/ใช้/เปิดเผยข้อมูล ซึ่งได้กระทำระหว่างที่ได้ให้ความยินยอมโดยชอบตาม พรบ.นี้

- กรณีที่การเพิกถอนความยินยอม **จะเกิดผลกระทบต่อเจ้าของข้อมูล** ผู้ควบคุมข้อมูลจะต้อง **แจ้งให้เจ้าของข้อมูลทราบ**ถึงผลกระทบนั้น

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิในการเข้าถึงและขอสำเนาข้อมูล (ดำเนินการภายใน 30 วัน)

1. เจ้าของข้อมูลฯมีสิทธิที่จะเข้าถึง(ขอดู) และขอรับสำเนาข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมข้อมูลฯรับผิดชอบอยู่
2. เจ้าของข้อมูลฯมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม

สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล

1. เจ้าของข้อมูลฯ**มีสิทธิขอรับข้อมูลของตนจากผู้ควบคุมข้อมูลฯ**ได้ในกรณีที่ผู้ควบคุมข้อมูลฯ จัดให้ข้อมูลฯนั้นอยู่ในรูปแบบที่อ่าน/ใช้งานทั่วไปและเปิดเผยได้อัตโนมัติด้วยเครื่องมือหรืออุปกรณ์(น่าจะหมายถึงด้วยวิธีการทางอิเล็กทรอกนิกส์)
2. เจ้าของข้อมูลฯมีสิทธิขอให้ผู้ควบคุมข้อมูลฯ **ส่งหรือโอนข้อมูล**ของตนในรูปแบบอัตโนมัติข้างต้น **ไปยังผู้ควบคุมข้อมูลฯรายอื่น** เมื่อกระทำได้ด้วยวิธีการอัตโนมัติ (น่าจะสอดคล้องกับระบบ NDID ที่ใช้พิสูจน์ตัวตน)
3. เจ้าของข้อมูลฯมี**สิทธิขอรับข้อมูลส่วนบุคคลของตน ที่ผู้ควบคุมข้อมูลฯส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลฯรายอื่น**โดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (ต่อ)

เจ้าของข้อมูลส่วนบุคคล มี**สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน** เมื่อใดก็ได้ ในกรณีดังต่อไปนี้

1. กรณีเป็นการเก็บรวบรวมได้โดยอาศัยเหตุไม่ต้องขอความยินยอม ตามมาตรา 24(4)หรือ(5) (ข้อยกเว้นด้วยเหตุ การปฏิบัติเพื่อประโยชน์สาธารณะ กับ เพื่อประโยชน์ของผู้ควบคุมข้อมูลฯเอง)
2. กรณีที่เป็นการเก็บรวบรวม/ใช้/เปิดเผย เพื่อวัตถุประสงค์เกี่ยวกับการตลาดโดยตรง
3. กรณีที่เป็นการ เก็บรวบรวม/ใช้/เปิดเผย เพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล เจ้าของข้อมูลฯมีสิทธิขอให้ผู้ควบคุมข้อมูลฯ ดำเนินการดังต่อไปนี้

1. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ หากว่าข้อมูลส่วนบุคคลนั้น **หมดความจำเป็น**ในการเก็บรักษาตามวัตถุประสงค์ที่เคยได้แจ้งไว้
2. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ เมื่อเจ้าของข้อมูล**ถอนความยินยอม**ในการเก็บรวบรวม/ใช้/เปิดเผย และผู้ควบคุมข้อมูลฯไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม/ใช้/เปิดเผยข้อมูลนั้นอีกต่อไป
3. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อเจ้าของข้อมูล**ใช้สิทธิคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลนั้น** และผู้ควบคุมข้อมูลฯไม่สามารถปฏิเสธคำคัดค้านนั้นได้
4. ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อข้อมูลส่วนบุคคลได้ถูก เก็บรวบรวม/ใช้/เปิดเผย **โดยไม่ชอบด้วยกฎหมาย**

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (ต่อ)

สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล

เจ้าของข้อมูลฯ มีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลฯ ระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีต่อไปนี้

1 กรณีที่**อยู่ระหว่างการตรวจสอบ** เมื่อเจ้าของข้อมูลขอให้ผู้ควบคุมข้อมูลฯดำเนินการให้ข้อมูลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด และผู้ควบคุมไม่ดำเนินการ ทำให้**เจ้าของข้อมูลร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ**

2 เมื่อข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ต้องลบ ทำลายเนื่องจากผู้ควบคุมข้อมูลฯ เก็บรวบรวม/ใช้/เปิดเผย โดยไม่ชอบด้วยกฎหมาย แต่**เจ้าของข้อมูลฯ ขอให้ระงับการใช้แทน**

3 เมื่อข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ แต่เจ้าของข้อมูลฯ**จำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย** ปฏิบัติตามหรือเป็นการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

4 เมื่อผู้ควบคุมข้อมูลฯอยู่ระหว่างการตรวจสอบข้อพิสูจน์ กรณี**ปฏิเสธคำคัดค้านของเจ้าของข้อมูลฯ** ตามมาตรา 32 (คัดค้านในการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล)

สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน

เจ้าของข้อมูลฯ ใช้สิทธิร้องขอให้ผู้ควบคุมข้อมูลฯ ต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้น **“ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด”** ได้

แบบบันทึกรายการเพื่อให้(เจ้าของข้อมูลส่วนบุคคล) ตรวจสอบ (มาตรา 39)

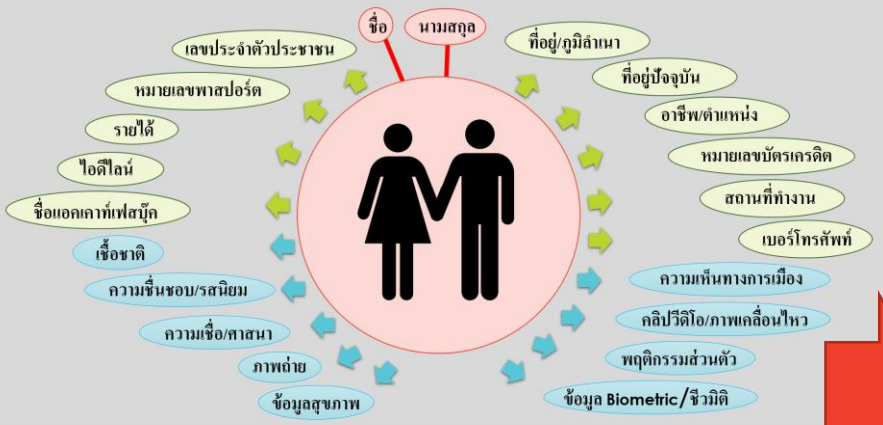
ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

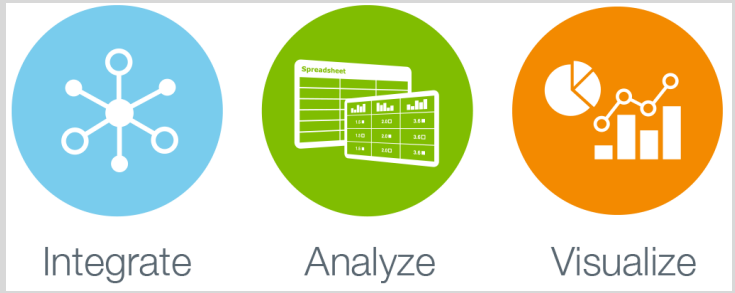
มีหน้าที่ต้องบันทึกรายการเกี่ยวกับข้อมูล เพื่อให้เจ้าของข้อมูลฯหรือสำนักงานคุ้มครองข้อมูลฯ ตรวจสอบได้ อย่างน้อย มีรายการ ดังต่อไปนี้

1. ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวม
2. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลแต่ละประเภท
3. ข้อมูลเกี่ยวกับ ผู้ควบคุมข้อมูลส่วนบุคคล
4. ระยะเวลาการเก็บรักษาข้อมูลฯ
5. สิทธิและวิธีการ เข้าถึงข้อมูลส่วนบุคคล และ เงื่อนไขของบุคคลที่มีสิทธิเข้าถึงข้อมูลและเงื่อนไขในการเข้าถึงข้อมูลนั้น
6. การใช้/เปิดเผยข้อมูล ตามมาตรา 27 วรรคสาม (การใช้/เปิดเผยข้อมูลที่ได้รับข้อยกเว้นไม่ต้องขอความยินยอม)
7. การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูล
8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1) (มาตรการความปลอดภัยในการเก็บรักษาข้อมูลส่วนบุคคล)

การละเมิดข้อมูลส่วนบุคคล PERSONAL DATA BREACH

บจก. กฎหมายและธุรกิจ อินเตอร์ คอนซัลแตนท์
Inter Consultants Law & Business Ltd.





ลักลอบเอาข้อมูลออกจากองค์กร

Identity Theft ขโมยตัวตนเพื่อสวมรอย

Profiling นำข้อมูลที่ประมวลผลไปใช้แสวงหาประโยชน์ทางการตลาด

Misuse นำไปใช้ในทางที่มิชอบ ขายข้อมูลเพื่อประโยชน์ทางธุรกิจ

Tracking Stalking ติดตาม สะกดรอย สอดแนม

การดำเนินการเมื่อเกิดการละเมิดข้อมูล (Data Breach)

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล

ดำเนินการสอบสวนเหตุที่เกิดขึ้น →

ประเภทข้อมูล/ปริมาณข้อมูล/เหตุที่เกิดการละเมิด/ผู้กระทำ

ดำเนินการแก้ไขอย่างเร่งด่วนที่สุด

ประเมินความเสี่ยงที่จะละเมิดสิทธิ/เสรีภาพเจ้าของข้อมูลหรือไม่ →

ประเมินความเสียหายที่(จะ)เกิดขึ้น

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach)

มีความเสี่ยงที่จะกระทบ
สิทธิ/เสรีภาพของบุคคลหรือไม่

72 ชั่วโมง

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

บริหารจัดการแก้ไขภายในองค์กร

- ข้อมูลของ Data Controller หรือ Data Processor
- วันเดือนปี ที่เกิดเหตุละเมิดข้อมูล
- รายละเอียดข้อมูลที่ถูกละเมิด เช่น ประเภทข้อมูล จำนวนข้อมูล
- ผลกระทบที่อาจเกิดจากการละเมิดข้อมูล
- ระดับความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- แนวทาง/วิธีการแก้ไข/จัดการกับการละเมิดข้อมูล

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ต้องแจ้งให้ทราบว่ามีการโอนข้อมูลไปยังต่างประเทศ

เจ้าของข้อมูลส่วนบุคคล
(Data Subject)

หลักการ :

- ประเทศปลายทางที่รับข้อมูล ต้องมีมาตรฐานด้าน Personal Data Protection ที่เพียงพอ (คณะกรรมการประกาศกำหนด)
- ส่ง/โอนข้อมูล ไปยังบริษัทในเครือเดียวกัน (จัดทำนโยบายที่ผูกพันบริษัทในเครือ) โดยนโยบายจะต้องได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล

ข้อยกเว้น การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

หลักการ :

- ประเทศปลายทางที่รับข้อมูล ต้องมีมาตรฐานด้าน Personal Data Protection ที่เพียงพอ (คณะกรรมการประกาศกำหนด)
- ส่ง/โอนข้อมูล ไปยังบริษัทในเครือเดียวกัน (จัดทำนโยบายที่ผูกพันบริษัทในเครือ) โดยนโยบายจะต้องได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล

การโอนข้อมูลไปต่างประเทศ อาจไม่ต้องพิจารณาหลักการนี้ก็ได้ หากว่า การส่งหรือโอนข้อมูลนั้น เป็นการดำเนินการเพื่อ

1. ปฏิบัติตามกฎหมาย(ของผู้ควบคุมข้อมูล)
2. ได้รับความยินยอมจากเจ้าของข้อมูลฯ ซึ่งผู้ควบคุมข้อมูลฯได้แจ้งให้ทราบถึงความมีมาตรฐานที่ไม่เพียงพอของประเทศหรือองค์กรฯปลายทางแก่เจ้าของข้อมูลแล้ว
3. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนทำสัญญานั้น
4. เป็นการทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับผู้อื่นเพื่อประโยชน์ของเจ้าของข้อมูลฯเอง
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างการหรือสุขภาพของเจ้าของข้อมูลฯหรือผู้อื่น เมื่อเจ้าของข้อมูลฯไม่สามารถให้ความยินยอมในขณะนั้นได้
6. เพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : Data Protection Officer (DPO)

ผู้ควบคุมข้อมูลส่วนบุคคล
Data Controller

การเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคลจำนวนมาก(ตามที่คณะกรรมการประกาศกำหนด)

ผู้ประมวลผลข้อมูลส่วนบุคคล
Data Processor

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล :
Data Protection Officer (DPO)

แจ้งต่อ

เจ้าของข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : Data Protection Officer (DPO)

- 1. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ (รวมถึงลูกจ้างหรือผู้รับจ้างของผู้ควบคุมฯหรือผู้ประมวลผลฯ) เกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- 2. ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลฯ หรือผู้ประมวลผลข้อมูลฯ เพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- 3. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีเกิดปัญหาเกี่ยวกับการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลฯ หรือ ผู้ประมวลผลข้อมูลฯ(รวมทั้งลูกจ้าง/ผู้รับจ้างของผู้ควบคุมฯหรือผู้ประมวลผลฯ)
- 4. รักษาความลับของข้อมูลส่วนบุคคลที่ตนได้ล่วงรู้/ได้มาจากการปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- 5. รับการติดต่อจากเจ้าของข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลและการใช้สิทธิของเจ้าของข้อมูลฯ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ความคุ้มครองตามกฎหมายของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล : Data Protection Officer (DPO)

(1) ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ ต้องอำนวยความสะดวกและสนับสนุนการปฏิบัติ หน้าที่ของ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (จัดหาเครื่องมือ/อุปกรณ์ และอำนวยความสะดวกในการเข้าถึงข้อมูลฯ)

(2) ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯ จะให้เจ้าหน้าที่คุ้มครองข้อมูลฯ ออกจากงานหรือเลิกสัญญาจ้าง เพราะเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลฯได้ปฏิบัติหน้าที่ตามกฎหมายนี้ ไม่ได้

(3) กรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลฯต้องสามารถรายงานไปยังผู้บริหารระดับสูงสุดของ ผู้ควบคุมข้อมูลฯหรือผู้ประมวลผลข้อมูลฯได้โดยตรง

(4) เจ้าหน้าที่คุ้มครองข้อมูลฯ อาจปฏิบัติหน้าที่หรือภารกิจงานอื่นได้ แต่ต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่คุ้มครองข้อมูลส่วนบุคคลตาม พรบ.นี้

การร้องเรียน กรณีข้อมูลส่วนบุคคลถูกใช้โดยมิชอบ หรือถูกละเมิด

ร้องเรียน

คณะกรรมการผู้เชี่ยวชาญ

1.รับเรื่องร้องเรียนจากเจ้าของข้อมูล กรณีผู้ควบคุมข้อมูลฯและผู้ประมวลผลข้อมูลฯ ฝ่าฝืน/ไม่ปฏิบัติตาม พรบ.นี้

2. พิจารณาเรื่องร้องเรียน ตามกฎหมายนี้

3. ตรวจสอบการกระทำของผู้ควบคุมข้อมูลฯและผู้ประมวลผลข้อมูลฯ เกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล

4. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

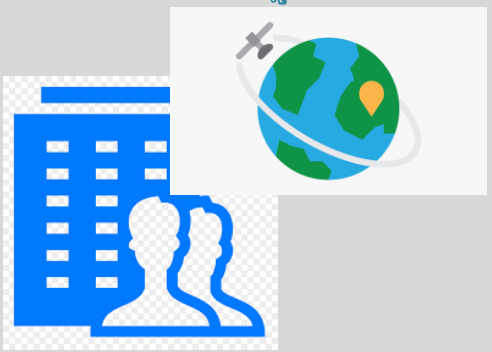
5. ปฏิบัติการอื่นๆตามที่คณะกรรมการมอบหมาย

การกำหนดขอบเขตการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สหกรณ์ออมทรัพย์ 1

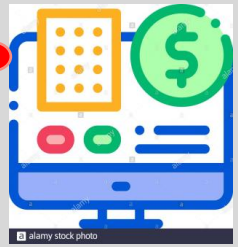
สหกรณ์ออมทรัพย์ 2

หน่วยงานของรัฐ



สถาบันการเงิน

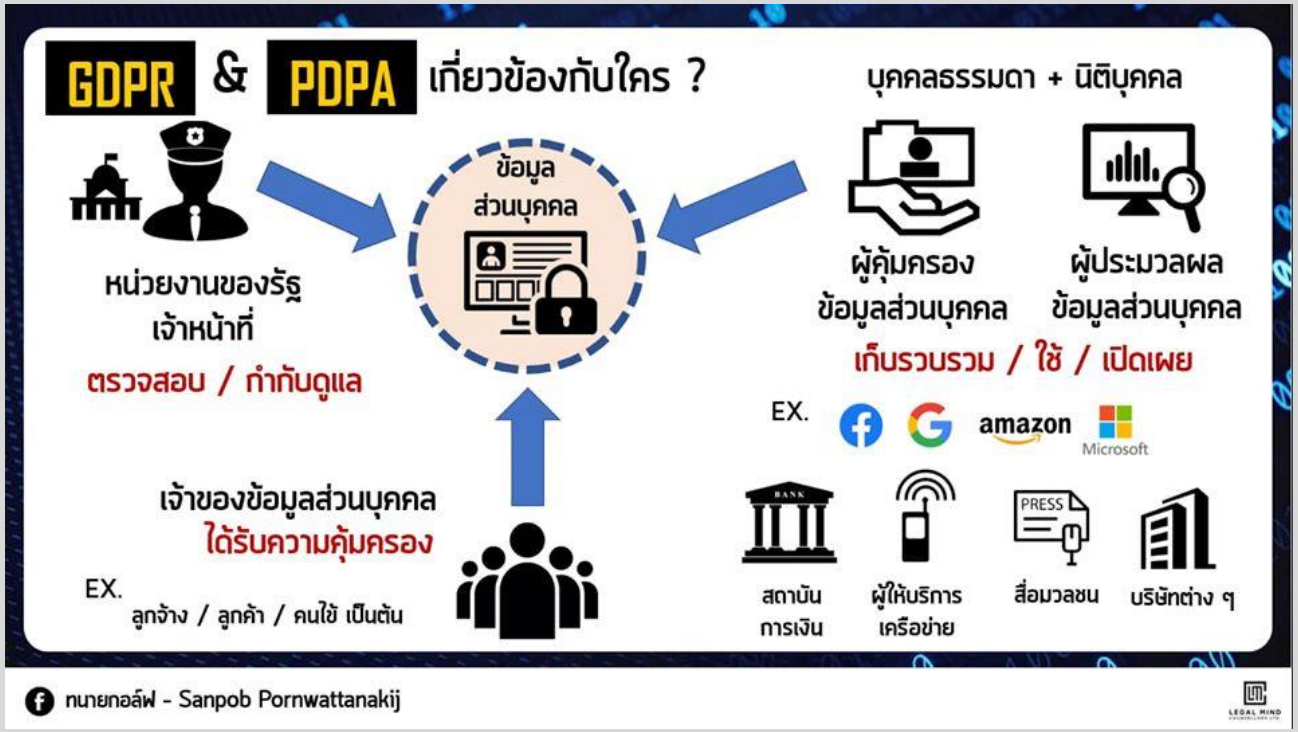
External Audit



Data Processor

PERSONAL DATA PROTECTION COMPLIANCE

การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

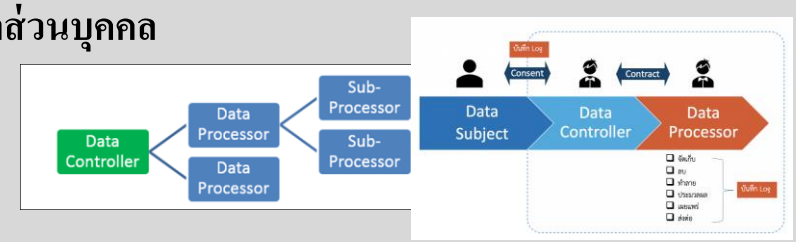


Scope of law

การกำหนดนโยบายด้านข้อมูลส่วนบุคคล
Personal Data Protection Policy

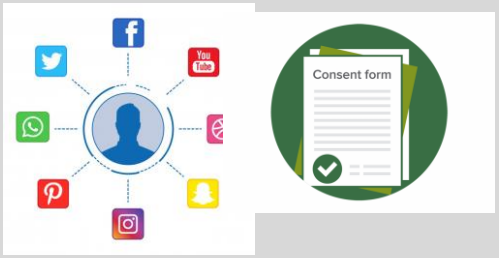
การคัดกรองและจัดแบ่งระดับข้อมูล
Data Mapping & Management

การกำหนดบทบาทและความรับผิดชอบข้อมูลส่วนบุคคล
Roles & Liabilities



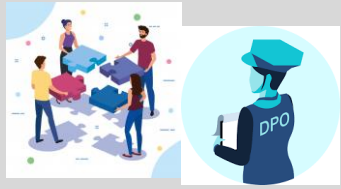
ประเมินความเสี่ยงและบริหารความเสี่ยงข้อมูลส่วนบุคคล
Personal Data Risk assessment

จัดทำช่องทางและแบบฟอร์มสำหรับเจ้าของข้อมูล
Data Subject' Channel & Consent form



กำหนดกระบวนการบริหารการละเมิดข้อมูลส่วนบุคคล
Flow & Guideline for Data Breach

จัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
Data Protection Officer Team



การกำหนดนโยบายด้านข้อมูลส่วนบุคคล Personal Data Protection Policy

ระบุสถานะขององค์กร/บริษัท
- Data Controller
- Data Processor
- Third Party

ระบุกิจกรรมขององค์กรที่ทำให้ต้องเก็บข้อมูลส่วนบุคคล
- วัตถุประสงค์กิจการ
- รูปแบบธุรกิจ
- ประเภทสินค้า/บริการ
- กลุ่มเป้าหมายของธุรกิจ

ระบุรูปแบบการเก็บข้อมูลส่วนบุคคล
- เอกสาร Hard Copy
- อิเล็กทรอนิกส์ Data
- ใช้ Outsourcing บริหารข้อมูล

ระบุกิจกรรมที่ดำเนินการกับข้อมูล
- การใช้ข้อมูลในวัตถุประสงค์ใด
- การประมวลผลข้อมูล
- การส่งให้ผู้ประมวลผลข้อมูลดำเนินการ
- การโอน/ส่งข้อมูลให้บริษัทในเครือต่างประเทศ
- การเปิดเผยข้อมูล/วิธีการเปิดเผย/เปิดเผยต่อใคร

ระบุมาตรการรักษาความปลอดภัยของข้อมูล
- การจัดชั้นความลับของข้อมูล
- การกำหนดระดับการเข้าถึงข้อมูล
- มาตรฐานด้าน IT ในการป้องกันการเจาะระบบ
- การซักซ้อมระบบป้องกันภัยทางไซเบอร์
- การสำรองข้อมูลที่ปลอดภัย

การคัดกรองและจัดแบ่งระดับข้อมูล Data Mapping & Management

รวบรวมข้อมูล

คัดกรองข้อมูล

บริหารจัดการข้อมูล

รักษาความปลอดภัยข้อมูล

การรวบรวมข้อมูล

บริษัท/องค์กร

เก็บข้อมูลส่วนบุคคลหรือไม่

YES

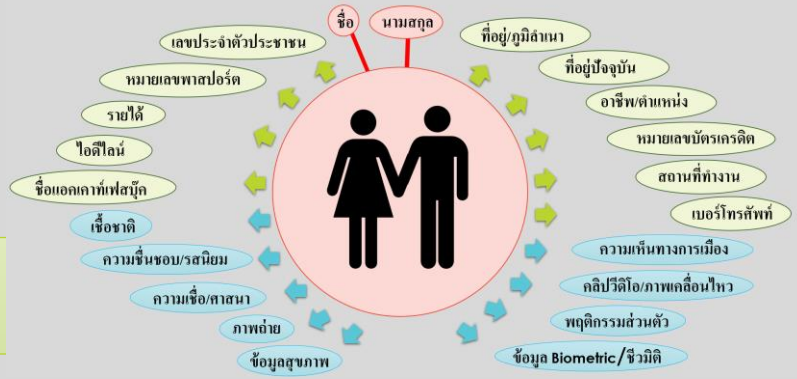
NO

เก็บข้อมูลกลุ่มบุคคลใด

- พนักงาน/ลูกจ้าง
- ลูกค้า
- Users ที่สนใจข้อมูล
- Vendor
- Supplier
- Business Partner

เก็บข้อมูลประเภท/Field ใดบ้าง

- Personal Data
- Sensitive Data



วัตถุประสงค์ในการเก็บข้อมูล

- Contract
- Legal Obligation

ต้องขอความยินยอมหรือไม่

- ยกเว้นไม่ต้องขอความยินยอม
- ต้องขอความยินยอม
  - ✓ ชัดแจ้ง
  - ✓ โดยปริยาย

ต้องประมวลผลข้อมูลหรือไม่

- ต้องวิเคราะห์/Analysis
- ใช้ข้อมูลดิบได้เลย

มีข้อมูลใดที่เก็บโดยไม่จำเป็น

- ไม่มี
- มี
  - ✓ ทำลาย/ลบ
  - ✓ ทำให้ระบุตัวไม่ได้

DATA MAPPING : รวบรวมข้อมูล (ขั้นที่ 1)

ข้อมูลที่กฎหมายกำหนด

ข้อมูลเก็บเพื่อประโยชน์ในการปฏิบัติตามกฎหมาย

ข้อมูลที่เก็บเพื่อประโยชน์อื่นๆในทางธุรกิจ

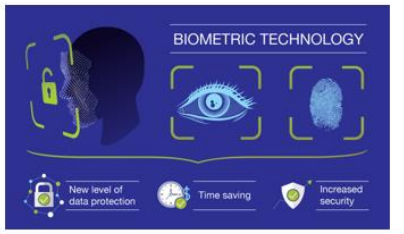
ข้อมูลที่เกินความจำเป็น
(หาวัตถุประสงค์ไม่ได้หรือไม่มีเหตุจะเก็บไว้)

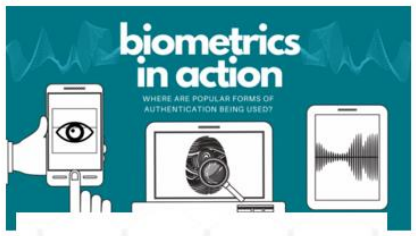
ส่งหรือโอนข้อมูลไปต่างประเทศ

DATA MAPPING : การแบ่งระดับข้อมูล

ข้อมูลเก็บเพื่อประโยชน์ในการปฏิบัติตามกฎหมาย

Sensitive Data?





การแจ้งรายละเอียด ในการเก็บ รวบรวม ข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลฯ **จะต้องแจ้งรายละเอียดในการเก็บรวบรวมข้อมูล**ส่วนบุคคล ให้แก่เจ้าของข้อมูลทราบ ก่อนหรือขณะเก็บรวบรวมข้อมูล ไม่ว่าจะต้องขอความยินยอมจากเจ้าของข้อมูลหรือไม่ก็ตาม (เว้นแต่เจ้าของข้อมูลจะได้ทราบถึงรายละเอียดนี้อยู่แล้ว)

- **วัตถุประสงค์**ในการเก็บรวบรวมข้อมูล เพื่อนำไปใช้หรือเปิดเผย
- แจ้งให้ทราบในกรณีที่เจ้าของข้อมูลฯ ต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมายหรือตามสัญญาหรือเพื่อเข้าทำสัญญา
- **ผลกระทบที่อาจเกิดขึ้น** กรณีที่เจ้าของข้อมูล **ไม่ให้เก็บหรือใช้**หรือเปิดเผยข้อมูล (ต้องไม่เป็นเงื่อนไขบังคับในการใช้บริการ)
- **เนื้อหา/ประเภทข้อมูล**ส่วนบุคคลที่จะเก็บรวบรวม
- **ระยะเวลา**ในการเก็บรักษาข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลต่อ**บุคคลภายนอก** (หน่วยงาน/บุคคลใดบ้าง)
- **ข้อมูลการติดต่อ** สถานที่ติดต่อ วิธีการติดต่อ ผู้ควบคุมข้อมูลส่วนบุคคล และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลฯ
- **แจ้งสิทธิของเจ้าของข้อมูลฯ**ตาม พรบ.นี้ (สิทธิถอนการยินยอม, ขอเข้าถึงและสำเนาข้อมูลของตน, ขอรับข้อมูลของตน, คัดค้านการเก็บ/ใช้/เปิดเผยข้อมูลของตน, ขอให้ลบหรือทำลายข้อมูลของตน, ขอให้ระงับการใช้ข้อมูลของตน, ร้องเรียนผู้ควบคุมข้อมูลที่ไม่ปฏิบัติตามคำร้องขอ, ร้องเรียนผู้ควบคุมที่ไม่ปฏิบัติตามกฎหมายนี้)

การเก็บ Sensitive Data (ข้อมูลส่วนบุคคลเชิงลึก)

หลักการ : ผู้ควบคุมข้อมูลฯจะต้อง **"ขอความยินยอมโดยชัดแจ้ง"** จากเจ้าของข้อมูลส่วนบุคคล หากจะทำการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลดังต่อไปนี้

- เชื้อชาติ/เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ/ศาสนา/ปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม (ต้องกระทำภายใต้การควบคุมของหน่วยงานรัฐที่มีอำนาจ)
- ข้อมูลสุขภาพ ความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม/ชีวภาพ (เกิดจากการใช้เทคโนโลยียืนยันตัวบุคคลจากลักษณะเด่นทางกายภาพหรือพฤติกรรม เช่น ลายนิ้วมือ ม่านตา จำลองใบหน้า เป็นต้น)
- ข้อมูลอื่นใดในทำนองเดียวกันกับข้างต้น (ภาพถ่ายหรือภาพเคลื่อนไหวของบุคคลก็จัดอยู่ในข้อมูลประเภทนี้)

DATA MAPPING : การคัดกรองข้อมูลที่ต้องขอความยินยอม

ข้อมูลที่เก็บเพื่อประโยชน์อื่นๆในทางธุรกิจ

ขอความยินยอมจากสมาชิก/ลูกค้า

หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล : การขอความยินยอม

- ผู้ควบคุมข้อมูลฯ มีหน้าที่ต้อง **ขอความยินยอม ก่อน หรือ ขณะ เก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล**จากเจ้าของข้อมูลฯ และจะต้องเก็บข้อมูลส่วนบุคคล**เท่าที่จำเป็น**จะต้องใช้ตามวัตถุประสงค์ที่มีเท่านั้น

แบบการขอความยินยอม ต้องขอโดย**ชัดแจ้ง** ด้วยวิธี**เป็นหนังสือ**หรือผ่าน**ระบบอิเล็กทรอนิกส์** (เว้นแต่โดยสภาพไม่อาจขอด้วยวิธีดังกล่าวได้)

- แจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลฯ
  - การขอความยินยอม ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน
    - มีวิธีการที่เข้าถึงได้ง่าย
      - ถ้อยคำและภาษาที่ใช้ต้องเข้าใจได้ง่าย ไม่ทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ของการขอความยินยอม (คณะกรรมการฯอาจกำหนดแบบและข้อความก็ได้)
        - การขอความยินยอม ต้องคำนึงถึง “อิสระของเจ้าของข้อมูลในการให้ความยินยอม” โดยต้องไม่มีเงื่อนไขบังคับให้ต้องยินยอม เพื่อเข้าถึงบริการหรือทำสัญญา

ห้ามไม่ให้ผู้ควบคุมข้อมูลฯ **เก็บรวบรวม ข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลฯโดยตรง เว้นแต่**

- ได้แจ้งเจ้าของข้อมูลส่วนบุคคลแล้วว่า ตนได้เก็บข้อมูลส่วนบุคคลจากแหล่งอื่น (ต้องแจ้งภายใน 30 วันนับแต่วันเก็บและต้องได้รับความยินยอม)
- เป็นการเก็บข้อมูลที่เข้าเหตุยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24(เหตุยกเว้น 6 ประการ) หรือ มาตรา 26 (เหตุยกเว้น Sensitive data)

DATA MAPPING : การคัดกรองข้อมูลส่วนบุคคลที่ไม่มีวัตถุประสงค์รองรับ

ข้อมูลที่เกินความจำเป็น

(หาวัตถุประสงค์ไม่ได้หรือไม่เพียงพอที่จะมีเหตุเก็บไว้)

ลบ ทำลาย หรือทำให้

ไม่สามารถระบุตัวได้

การกำหนดบทบาทและความรับผิดชอบข้อมูลส่วนบุคคล Roles & Liabilities

บทบาทระดับธุรกิจ/กิจการ

นโยบายข้อมูลส่วนบุคคลสำหรับองค์กร
กำหนดข้อบังคับให้ส่วนงานในองค์กร
ต้องมีแนวทางเดียวกัน

สหกรณ์ออมทรัพย์ 1

External Audit

ข้อตกลงกำหนดขอบเขตในการรับข้อมูล
ข้อตกลงห้ามเปิดเผย/ส่ง/โอนข้อมูลต่อโดยไม่ได้รับอนุญาต
ความรับผิดกรณีละเมิดข้อตกลง

Data Processor

ข้อตกลงกำหนดขอบเขตในการรับข้อมูล
ข้อตกลงกำหนดขอบเขตในการประมวลผลข้อมูล
ความรับผิดกรณีละเมิดข้อตกลง

สหกรณ์ออมทรัพย์ 2

หน่วยงานของรัฐ

ข้อตกลงกำหนดขอบเขตในการรับข้อมูล
ข้อตกลงกำหนดขอบเขตในการใช้ข้อมูล
ข้อตกลงในการรักษาความปลอดภัยข้อมูล
ความรับผิดกรณีละเมิดข้อตกลง

แจ้งนโยบายคุ้มครองข้อมูลขององค์กรให้ทราบ

สถาบันการเงิน

แจ้งนโยบายคุ้มครองข้อมูลขององค์กรให้ทราบ

การกำหนดบทบาทและความรับผิดชอบข้อมูลส่วนบุคคล Roles & Liabilities

บทบาทระดับองค์กร

Adminstrative

ผู้เก็บ/รวบรวมข้อมูลส่วนบุคคล

สมาชิก/ลูกค้า

Human Resource

ผู้เก็บ/รวบรวมข้อมูลส่วนบุคคล

พนักงาน/ลูกจ้างชั่วคราว

Vendor/Supplier

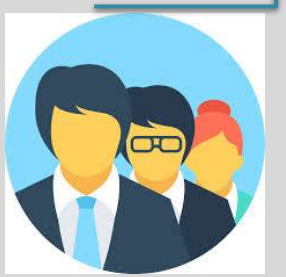
ผู้เก็บ/รวบรวมข้อมูลส่วนบุคคล

จัดซื้อจัดจ้าง

IT

ผู้ควบคุม/ดูแลระบบจัดเก็บข้อมูลส่วนบุคคล

ผู้กำกับดูแล มาตรการรักษาความปลอดภัยระบบ



Legal

ร่างนโยบาย/ข้อตกลง/สัญญา

ให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

Compliance

ผู้กำกับ/ดูแลการปฏิบัติตามกฎหมายขององค์กร

ผู้กำกับ/ดูแลการปฏิบัติตามนโยบายขององค์กร

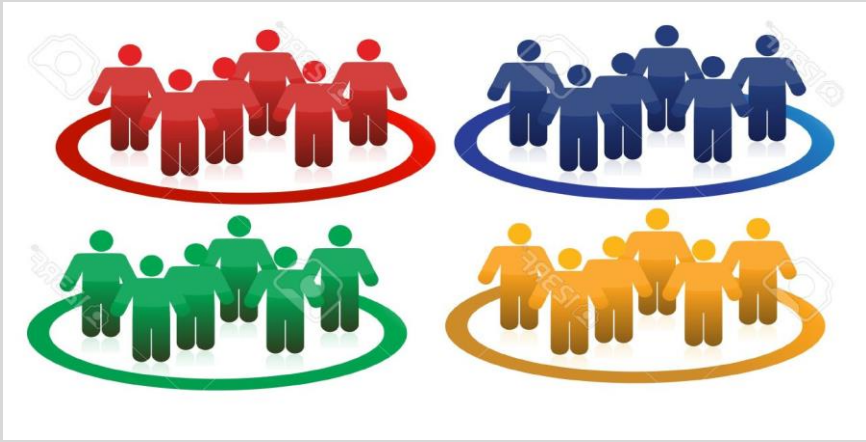
การประเมินความเสี่ยงและบริหารความเสี่ยงข้อมูลส่วนบุคคล Personal Data Risk assessment

เป้าหมายของการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล

เพื่อหา**กลุ่มบุคคล**ที่มีโอกาสเสี่ยงที่ข้อมูลจะถูกละเมิด

เพื่อหา**กลุ่มข้อมูล**ที่มีโอกาสเสี่ยงที่ข้อมูลจะถูกละเมิด

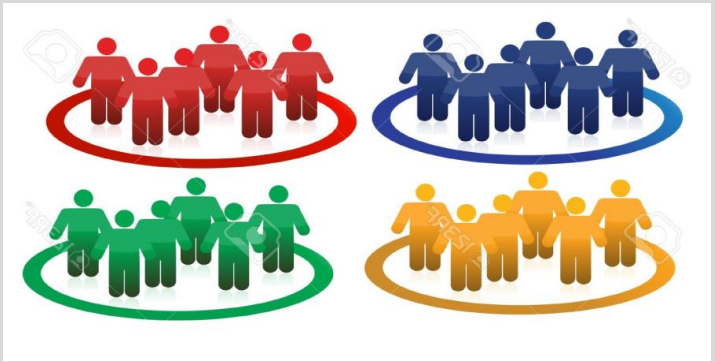
เพื่อหา**ช่องทางหรือรูปแบบ**ที่เสี่ยงในการถูกใช้เพื่อละเมิดข้อมูล



เพื่อหามาตรการป้องกันและบรรเทาความเสี่ยงที่อาจจะเกิดขึ้น

ความเสี่ยง : กลุ่มบุคคลที่มีโอกาสเสี่ยงที่ข้อมูลจะถูกละเมิด

บริษัทเก็บข้อมูลส่วนบุคคลของกลุ่มบุคคลใดบ้าง



กลุ่มบุคคลใด เป็นหัวใจหลัก
ในการขับเคลื่อนองค์กร/ธุรกิจ

สมาชิก
ลูกค้า
พนักงานประจำ

ข้อมูลของกลุ่มบุคคลใด เป็นที่
ต้องการในธุรกิจ/เศรษฐกิจ

สมาชิก
ลูกค้า

กลุ่มบุคคลใด โอกาสจะทำให้ข้อมูล
ส่วนบุคคลรั่วไหลออกจากองค์กร

Agent Company
Business Partner

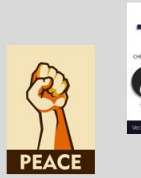
ข้อมูลของบุคคลใด ที่หากรั่วไหลออกไป
จะสร้างความเสียหายให้แก่องค์กรมากที่สุด

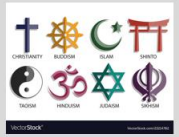
สมาชิก
ลูกค้า

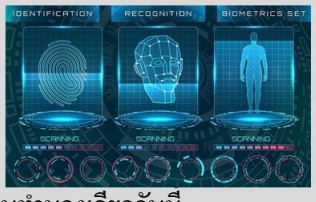
ความเสี่ยง : เพื่อหากลุ่มข้อมูลที่มีโอกาสเสี่ยงที่ข้อมูลจะถูกละเมิด

บริษัทเก็บข้อมูลส่วนบุคคลประเภทใดบ้าง

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ/ชีวมิติ
- ข้อมูลอื่นๆที่กระทบต่อเจ้าของข้อมูลในทำนองเดียวกันนี้ (คณะกรรมการประกาศกำหนด)







ข้อมูลใดที่ทำให้ระบุตัวบุคคลได้มากที่สุด

ข้อมูลใดที่เป็นที่ต้องการของธุรกิจมากที่สุด

ข้อมูลใดที่ได้มายากที่สุด

ข้อมูลใดที่ระบบป้องกันเบาบางที่สุด

ข้อมูลใดที่เคยถูก Hack บ่อยที่สุด

ข้อมูลใดมีมูลค่าความเสียหายสูงสุด

ความเสี่ยง : เพื่อหาช่องทางหรือรูปแบบที่เสี่ยงในการถูกใช้เพื่อละเมิดข้อมูล

บริษัทมีรูปแบบการเก็บข้อมูล/แหล่งเก็บข้อมูลอย่างไรบ้าง

ระบบ IT/Computer

ระบบเอกสาร

- ระบบ IT มีมาตรฐานรับรองความปลอดภัยหรือไม่ ระดับใด
- ระบบ IT เคยถูกเจาะข้อมูลจากภายนอกโดยไม่สามารถป้องกันได้หรือไม่
- มีการเก็บข้อมูล IT สำรองไว้ในอีกแห่งหนึ่งหรือไม่
- มีการจัดชั้นความลับ+เข้ารหัสก่อนถึงข้อมูลหรือไม่
- ระบบเอกสาร มีการเก็บรักษาในสภาพแวดล้อมที่เหมาะสมหรือไม่
- มีระบบการสืบค้นเอกสารที่รวดเร็ว/แมนยำ หรือไม่
- มั่นใจได้อย่างไรว่า เอกสารยังคงอยู่ครบถ้วนในสภาพที่ใช้งานได้

ผลลัพธ์จากการประเมินความเสี่ยง = มาตรการบรรเทา/ป้องกันความเสี่ยง

กำหนดมาตรการรักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคลของ**ลูกค้า** เข้มข้นกว่าข้อมูลส่วนบุคคลของกลุ่มบุคคลอื่น

- จัดเก็บข้อมูลลูกค้าโดยแยกข้อมูล**ชื่อ**ออกจากข้อมูลอื่นๆ และใช้ **Code** แทนชื่อใน **Profile** ลูกค้าทุกราย
- กำหนดชั้นความลับสำหรับบุคลากรที่จะเข้าถึงข้อมูล ชื่อ ของลูกค้า และกำหนดให้รหัสเข้าถึงข้อมูลเปลี่ยนทุกวัน
- กำหนดให้ข้อมูล หมายเลขบัตรเครดิต/ข้อมูลสุขภาพ เป็นข้อมูลที่ต้องปกป้องอย่างเข้มข้นที่สุด

- มีระบบการMonitor การส่งข้อมูลจากคอมพ์พนักงานไปสู่ภายนอกและมีระบบ Block การส่งข้อมูลที่รวดเร็วเมื่อพบความผิดปกติ
- จัดทำข้อตกลงที่กำหนดความรับผิดระดับสูงสำหรับคู่ค้า/ผู้ประมวลผลที่รับข้อมูลลูกค้าไปดำนินการตามสัญญา

จัดทำช่องทางและแบบฟอร์มสำหรับเจ้าของข้อมูล Data Subject' Channel & Consent form

ช่องทางในการขายสินค้า หรือ ให้บริการ

ช่องทางการเก็บ รวบรวม ข้อมูลส่วนบุคคล

ช่องทางในการขอความยินยอม

ช่องทางการขอความยินยอมจากเจ้าของข้อมูล

ตัวอย่างการแบบขอความยินยอม

Box 1

Company A ใช้คุกกี้ในการให้บริการและปรับปรุงบริการของเรา เพื่อเพิ่มประสิทธิภาพการเรียกดูข้อมูลของท่าน กรณีที่ท่านใช้งานเว็บไซต์นี้ต่อไป ถือว่าท่านได้ยินยอมให้มีการใช้งานคุกกี้ ยืนยัน

คุ๊กกี้ คืออะไร

Box 2

เราใช้คุกกี้ (cookie) เพื่อพัฒนาประสบการณ์การใช้งานจากการเยี่ยมชมเว็บไซต์ของเราและเพื่อสนับสนุนประสิทธิภาพในการนำเสนอข้อมูลและเนื้อหาต่างๆ ที่ผู้เข้าใช้งานจะได้รับชม

โดยทางบริษัทจะสร้างไฟล์ข้อมูลที่มีขนาดเล็กไว้ในอินเตอร์เน็ตเบราว์เซอร์ของผู้เข้าใช้งาน เพื่อเก็บและจดจำความสนใจของผู้เข้าใช้งาน เพื่อพัฒนาให้มีการแสดงผลที่สอดคล้องกับความชื่นชอบและความสนใจในการใช้งาน และเพื่อพัฒนาประสิทธิภาพในการแสดงผลของข้อมูล และเพื่อวิเคราะห์และนำเสนอโฆษณา รวมถึงเพื่ออำนวยความสะดวกในการให้บริการต่างๆ ภายในเว็บไซต์ของเรา และเมื่อผู้เข้าใช้งานกลับมาเยี่ยมชมหรือกลับเข้ามาใช้บริการในครั้งต่อไป แต่การเก็บข้อมูลด้วยคุกกี้จะไม่ระบุตัวตนของผู้เข้าใช้งาน

ทั้งนี้เพื่อทำการวิเคราะห์ซึ่งอาจทำหรือให้บริการโดยบุคคลอื่นที่ให้บริการหรือได้รับมอบหมายให้กระทำแทนในนามของ..... เช่น Google Analytic เป็นต้น

เมื่อผู้เข้าใช้งานมีการกลับมาเยี่ยมชมเว็บไซต์โดยไม่เปลี่ยนแปลงการตั้งค่าคุกกี้บนอินเตอร์เน็ตเบราส์เซอร์อุปกรณ์ของผู้ใช้งานจะยอมรับคุกกี้อัตโนมัติในการเข้าใช้งานในครั้งต่อไป ซึ่งถ้าหากผู้เข้าใช้งานไม่ต้องการให้คุกกี้ทำการรวบรวมข้อมูล ผู้ใช้งานสามารถเลือกเปลี่ยนแปลง หรือตั้งค่า google analytic เป็นต้น

เมื่อผู้เข้าใช้งานมีการกลับมาเยี่ยมชมเว็บไซต์โดยไม่เปลี่ยนแปลงการตั้งค่าคุกกี้บนอินเตอร์เน็ตเบราส์เซอร์อุปกรณ์ของผู้ใช้งานจะยอมรับคุกกี้อัตโนมัติในการเข้าใช้งานในครั้งต่อไป ซึ่งถ้าหากผู้เข้าใช้งานไม่ต้องการให้คุกกี้ทำการรวบรวมข้อมูล ผู้ใช้งานสามารถเลือกเปลี่ยนแปลง หรือตั้งค่าการยอมรับคุกกี้ได้ที่เมนู "การตั้งค่า" ของอินเตอร์เน็ตเบราว์เซอร์ที่ใช้งานอยู่

เนื่องจากการเข้าเวปไซต์เพื่อทำธุรกรรมในครั้งนี้ มีการเก็บ ข้อมูลส่วนบุคคลของท่าน เพื่อการใช้บริการ Company..... บริษัทจึงขอแจ้งให้ท่านทราบถึงนโยบายและยินยอมให้เก็บ รวบรวม และใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ในการให้บริการอย่างดีที่สุด ยินยอม

นโยบายด้านข้อมูลส่วนบุคคล

Box 3

นโยบายข้อมูลส่วนบุคคล และ แบบขอความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล

บริษัท .....ให้ความสำคัญอย่างยิ่ง ในการรักษาความปลอดภัยในการเก็บรักษาข้อมูลส่วนบุคคลของลูกค้ารวมถึงพนักงานและบุคลากรของบริษัทฯ ประกอบกับบริษัทฯ มีความมุ่งมั่นที่จะปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ประกอบการที่เก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลให้มีประสิทธิภาพ บริษัทฯ จึงได้กำหนดนโยบายเพื่อรองรับการปฏิบัติตามกฎหมายดังนี้

บริษัทได้เก็บ รวบรวม ใช้ ประมวลผล หรือเปิดเผย ข้อมูลส่วนบุคคลของท่าน ภายใต้สิทธิและเงื่อนไขตามหนังสือยินยอมฉบับนี้ ซึ่งได้แก่ **ข้อมูลส่วนบุคคล** ดังต่อไปนี้

1. ชื่อ 2. นามสกุล 3. สำเนา/ภาพถ่ายบัตรประจำตัวประชาชนหรือหนังสือเดินทางหรือบัตรที่ออกโดยหน่วยราชการและข้อมูลที่ปรากฏตามบัตรวัน เดือน ปี เกิด 4. ที่อยู่ 5. หมายเลขโทรศัพท์ติดต่อ/อีเมล์ 6. อาชีพ

ข้อมูลส่วนบุคคลตามมาตรา 26 (Sensitive Data) ดังต่อไปนี้

1. ข้อมูลภาพถ่าย 2. ข้อมูลชีวมิติ(ใบหน้า)

วัตถุประสงค์ในการเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคล บริษัทฯ ดำเนินการเพื่อวัตถุประสงค์ ดังต่อไปนี้

- เพื่อประโยชน์ในการยืนยันตัวตนและปฏิบัติตามกฎหมาย ข้อบังคับ หรือระเบียบ ประกาศของหน่วยงานกำกับดูแลตามกฎหมาย ได้แก่
- เพื่อเป็นหลักฐานทางกฎหมายในการทำนิติกรรมหรือธุรกรรมการซื้อขาย แลกเปลี่ยน เงินตราต่างประเทศ
- เพื่อประโยชน์ในการรับสิทธิประโยชน์ ข่าวสาร ประชาสัมพันธ์ เชิญชวนเข้าร่วมกิจกรรม รับทราบข้อมูลเกี่ยวกับธุรกิจ เสนอสิทธิหรือประโยชน์หรือโอกาสในการใช้บริการ ได้รับสิทธิหรือสิ่งของสมนาคุณ
- เพื่อเสนอบริการหรือผลิตภัณฑ์ของบริษัทฯ
- เพื่อรับฟังความคิดเห็นเพื่อปรับปรุงพัฒนา การบริการและผลิตภัณฑ์ของบริษัทฯ
- เพื่อการดำเนินการอื่นๆที่เกี่ยวข้องกับวัตถุประสงค์ที่กล่าวมาข้างต้น

ตัวอย่างการแบบขอความยินยอม (ต่อ)

ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ จะไม่เก็บรักษาข้อมูลส่วนบุคคลของลูกค้า เกินกว่าระยะเวลาที่กฎหมายกำหนด และระยะเวลาการเรียกร้องสิทธิหรืออายุความฟ้องร้องดำเนินคดีในทางแพ่ง (10 ปี)

กรณีข้อมูลส่วนบุคคลตามมาตรา 26(ข้อมูลที่มีความอ่อนไหว) ประเภทภาพถ่าย ข้อมูลชีวมิติ บริษัทฯ มีระยะเวลาการเก็บรักษาไว้ ..... วัน นับแต่วันที่เก็บ รวบรวมข้อมูล

การเปิดเผยข้อมูลส่วนบุคคล

บริษัทฯ จะไม่เปิดเผยข้อมูลส่วนบุคคลของลูกค้าต่อบุคคลอื่น เว้นแต่เป็นการเปิดเผยเพื่อการปฏิบัติตามกฎหมายที่บริษัทฯ มีหน้าที่ต้องปฏิบัติตามอย่างเคร่งครัด และ เพื่อดำเนินการประมวลผลข้อมูลเพื่อประโยชน์ทางการตลาดและการส่งเสริมการขาย ซึ่งเป็นการส่งข้อมูลเพื่อให้ผู้ประมวลผลดำเนินการ

สิทธิต่างๆของเจ้าของข้อมูล

เมื่อท่านได้ให้ความยินยอมในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลต่อบริษัทแล้ว ท่านมีสิทธิดังต่อไปนี้ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- สิทธิในการขอถอนความยินยอม เจ้าของข้อมูลฯ จะเพิกถอนการยินยอมให้ใช้หรือเปิดเผยข้อมูลเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิห้ามเพิกถอนตามกฎหมายหรือตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลฯ ทั้งนี้ การเพิกถอนการยินยอม ไม่กระทบต่อการเก็บ/ใช้/เปิดเผยข้อมูล ซึ่งได้กระทำระหว่างที่ได้ให้ความยินยอมโดยชอบและบริษัทฯ จะต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบที่อาจเกิดขึ้นเมื่อมีการถอนความยินยอม
- สิทธิในการเข้าถึงและขอสำเนาข้อมูล เจ้าของข้อมูลฯ มีสิทธิที่จะเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนที่บริษัทฯ รับผิดชอบอยู่และมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม
- สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล เจ้าของข้อมูลฯ มีสิทธิขอรับข้อมูลของตนจากบริษัทฯ ได้ ในกรณีที่บริษัทฯ จัดให้ข้อมูลนั้นอยู่ในรูปแบบที่อ่าน/ใช้งานทั่วไปและเปิดเผยได้อัตโนมัติด้วยเครื่องมือหรืออุปกรณ์ และเจ้าของข้อมูลฯ มีสิทธิขอให้บริษัทฯ **ส่งหรือโอนข้อมูล**ของตนในรูปแบบอัตโนมัติข้างต้น ไปยังผู้ควบคุมข้อมูลฯ รายอื่น เมื่อกระทำได้ด้วยวิธีการอัตโนมัติและเจ้าของข้อมูลฯ มีสิทธิขอรับข้อมูลส่วนบุคคลของตนที่บริษัทฯ ส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลฯ รายอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้
- สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน เจ้าของข้อมูลส่วนบุคคล มีสิทธิที่จะคัดค้านมิให้บริษัทฯ เก็บรวบรวม ใช้ ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลได้ เว้นแต่เป็นการดำเนินการที่บริษัทฯ ต้องปฏิบัติตามกฎหมาย
- สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล เจ้าของข้อมูลฯ มีสิทธิขอให้ผู้ควบคุมข้อมูลฯ ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ หากว่าข้อมูลส่วนบุคคลนั้นหมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ที่เคยได้แจ้งไว้ หรือดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น ไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ เมื่อเจ้าของข้อมูลถอนความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผย และผู้ควบคุมข้อมูลฯ ไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นอีกต่อไป หรือดำเนินการลบ ทำลาย หรือทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ เมื่อเจ้าของข้อมูลใช้สิทธิคัดค้านการเก็บรวบรวมใช้เปิดเผยข้อมูลนั้น และผู้ควบคุมข้อมูลฯ ไม่สามารถปฏิเสธคำคัดค้านนั้นได้ หรือดำเนินการลบ ทำลาย หรือทำให้ข้อมูลนั้น เมื่อข้อมูลส่วนบุคคลได้ถูก เก็บ รวบรวม ใช้ เปิดเผยโดยไม่ชอบด้วยกฎหมาย

- สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล เจ้าของข้อมูลฯ มีสิทธิที่จะขอให้บริษัทฯ ระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีที่อยู่ระหว่างการตรวจสอบ เมื่อเจ้าของข้อมูลขอให้บริษัทฯ ดำเนินการให้ข้อมูลนั้นถูกต้อง เป็นปัจจุบัน หรือเมื่อข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ต้องลบ ทำลาย แต่เจ้าของข้อมูลฯ ขอให้ระงับการใช้แทนการลบ ทำลาย หรือเมื่อข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ แต่เจ้าของข้อมูลฯ จำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย หรือเมื่อบริษัทฯ อยู่ระหว่างการตรวจสอบข้อพิสูจน์ กรณีปฏิเสธคำคัดค้านของเจ้าของข้อมูลฯ เรื่องการคัดค้านในการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล
- สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน
เจ้าของข้อมูลฯ ใช้สิทธิร้องขอให้บริษัทฯ ดำเนินการให้ข้อมูลส่วนบุคคลนั้น ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิดได้

ช่องทางในการใช้สิทธิ

บริษัทฯ จัดให้มีช่องทางในการที่ท่านจะใช้สิทธิได้ ดังนี้

(1) วิธีการขอความยินยอมโดยขอเป็นหนังสือ ณ สำนักงานหรือสาขาที่ให้บริการของบริษัทฯ

(2) วิธีการขอความยินยอมผ่านระบบอิเล็กทรอนิกส์ โดยผ่านเว็บไซต์ของบริษัทฯ

การติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หากท่านมีข้อสงสัย หรือต้องการสอบถามเกี่ยวกับนโยบายและการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ หรือประสงค์จะสอบถามเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูลในการดำเนินการอย่างหนึ่งอย่างใดกับข้อมูลส่วนบุคคลของท่านซึ่งบริษัทฯได้เก็บ รวบรวม ใช้ หรือเปิดเผย ท่านสามารถติดต่อได้ที่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล บริษัท ซุปเปอร์ริช เคอเรนซี่ เอ็กซ์เชนจ์ (1965) จำกัด

สถานที่ติดต่อ สำนักงาน .....

โทร.

ข้าพเจ้าทราบถึงนโยบายและความจำเป็นตลอดจนวัตถุประสงค์และสิทธิต่างๆในการเก็บข้อมูลส่วนบุคคลของบริษัท ..... **แล้ว จึงได้ให้ความยินยอมในการเก็บข้อมูลส่วนบุคคล**

กรณีที่ไม่ยินยอม บริษัทฯไม่สามารถนำข้อมูลส่วนบุคคลของข้าพเจ้าไปใช้ในวัตถุประสงค์อื่นได้ นอกเหนือไปจากวัตถุประสงค์เพื่อการปฏิบัติตามกฎหมายที่ระบุไว้

ยินยอม ไม่ยินยอม

ช่องทางการขอเพิกถอนความยินยอม

รูปแบบการขอความยินยอม : Consent Form

ชัดแจ้ง (แยกออกจากส่วนอื่นๆของสัญญาหรือข้อชี้แจงต่างๆ)

มีช่องทางให้ยินยอมได้สอดคล้องกับการเก็บข้อมูล และไม่บังคับให้ต้องยินยอม

แจ้งวัตถุประสงค์ในการเก็บ รวบรวม ใช้ และระยะเวลาในการเก็บข้อมูล

เมื่อขณะให้ความยินยอม สะดวก และชัดแจ้งอย่างไร

การเพิกถอนความยินยอม ต้องสะดวก และชัดแจ้งเช่นเดียวกัน

แบบขอเพิกถอนความยินยอม

ส่วนที่ 1 ข้อมูลเกี่ยวกับผู้ขอใช้สิทธิ

1. คำนำหน้าชื่อ* ○นาย ○นาง ○นางสาว
2. ชื่อ (ภาษาไทย)* ..... นามสกุล (ภาษาไทย)* .....
   (English) ..... (English) .....
3. เลขที่สัญญา/เลขที่อ้างอิงผู้ใช้บริการ/รหัสลูกค้า* .....
4. หมายเลขโทรศัพท์ติดต่อกลับ* ..... E-mail*.....

ส่วนที่ 2 การแจ้งสิทธิของเจ้าของข้อมูล

ในกรณีที่ท่านเป็น เจ้าของข้อมูลส่วนบุคคล ซึ่งเคยได้ให้ข้อมูลส่วนบุคคลของท่านแก่บริษัทฯ โดยท่านมีความประสงค์จะขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทซึ่งเป็น "ผู้ควบคุมข้อมูลส่วนบุคคล" ขอแจ้งกระบวนการใช้สิทธิของท่านดังนี้

ประเภทสิทธิที่เจ้าของบุคคลสามารถร้องขอได้ มีดังต่อไปนี้

2.1 สิทธิในการขอถอนความยินยอม

เมื่อได้ให้ยินยอมแล้ว เจ้าของข้อมูลส่วนบุคคล จะเพิกถอนการยินยอมให้ใช้หรือเปิดเผยข้อมูลเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิห้ามเพิกถอน ตามกฎหมายหรือตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ทั้งนี้ การเพิกถอนการยินยอม ไม่กระทบต่อการเก็บ/ใช้/เปิดเผยข้อมูล ซึ่งได้กระทำระหว่างที่ได้ให้ความยินยอมโดยชอบและ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบถึงผลกระทบที่อาจเกิดขึ้นเมื่อมีการถอนความยินยอม

2.2 สิทธิในการเข้าถึงและขอสำเนาข้อมูล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิที่จะเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมข้อมูลรับผิดชอบอยู่ และมีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม

2.3 สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอรับข้อมูลของตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้ข้อมูลนั้นอยู่ในรูปแบบที่อ่าน/ใช้งานทั่วไปและเปิดเผยได้อัตโนมัติด้วย เครื่องมือหรืออุปกรณ์และ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ส่งหรือโอนข้อมูลของตนในรูปแบบอัตโนมัติข้างต้น ไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น เมื่อกระทำได้ด้วยวิธีการอัตโนมัติ และ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลของตน ที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

ตัวอย่างการแบบขอถอนความยินยอม (ต่อ)

อนึ่ง การใช้สิทธิข้อนี้ เจ้าของข้อมูลส่วนบุคคล ต้องให้ความยินยอมโดยชัดแจ้งในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ซึ่งไม่อยู่ในหลักการตามนโยบายของบริษัทฯ

2.4 สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน

เจ้าของข้อมูลส่วนบุคคล มีสิทธิที่จะคัดค้านมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ ประมวลผล หรือเปิดเผยข้อมูลส่วนบุคคลได้ เว้นแต่เป็นการดำเนินการที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมาย และเป็นกรณี การเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคลนั้นเพื่อเก็บเป็นพยานหลักฐานสำหรับการดำเนินคดีที่อาจเกิดขึ้นระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับลูกค้าภายในอายุความแห่งกฎหมาย

2.5 สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ หากว่าข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ที่เคยได้แจ้งไว้ หรือ ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้ เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผย และผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นอีกต่อไป หรือ ดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการเก็บรวบรวม ใช้เปิดเผยข้อมูลนั้น และผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถปฏิเสธคำคัดค้านนั้นได้ หรือดำเนินการลบ ทำลาย หรือ ทำให้ข้อมูลนั้น เมื่อข้อมูลส่วนบุคคลได้ถูก เก็บรวบรวม ใช้ เปิดเผย โดยไม่ชอบด้วยกฎหมาย ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจคัดค้านการใช้สิทธินี้ ถ้าการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล เป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพื่อปฏิบัติตามกฎหมาย หรือเป็นกรณีเพื่อเก็บเป็นพยานหลักฐานสำหรับการดำเนินคดีที่อาจเกิดขึ้นระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับลูกค้าภายในอายุความแห่งกฎหมาย

2.6 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีที่อยู่ระหว่างการตรวจสอบ เมื่อเจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด และบริษัทฯยังไม่ดำเนินการ ทำให้เจ้าของข้อมูลส่วนบุคคลร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ หรือ เมื่อข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ต้องลบ ทำลายเนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม/ใช้/เปิดเผย โดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทนการลบ ทำลาย หรือเมื่อข้อมูลส่วนบุคคลนั้น หมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ แต่เจ้าของข้อมูลส่วนบุคคลจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย ปฏิบัติตามหรือเป็นการใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ระหว่างการตรวจสอบข้อพิสูจน์ กรณีปฏิเสธคำคัดค้านของเจ้าของข้อมูลส่วนบุคคล เรื่องการคัดค้านในการเก็บรวบรวม/ใช้/เปิดเผย ข้อมูลส่วนบุคคล

2.7 สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน

เจ้าของข้อมูลส่วนบุคคล ใช้สิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลส่วนบุคคลนั้น ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิดได้

2.8 สิทธิในการยื่นเรื่องร้องเรียน

เมื่อเจ้าของข้อมูลส่วนบุคคล ได้ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการตามสิทธิต่างๆข้างต้น แต่ปรากฏว่า ผู้ควบคุมข้อมูลส่วนบุคคล ปฏิเสธ หรือ ไม่ดำเนินการตามคำร้องขอ เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ยื่นเรื่องร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่ท่านเชื่อว่า ผู้ควบคุมข้อมูลส่วนบุคคล ไม่ดำเนินการอันเป็นการปฏิบัติโดยไม่ชอบด้วยกฎหมาย

ส่วนที่ 3 ขั้นตอนการดำเนินการหลังจากท่านแจ้งความประสงค์ของใช้สิทธิ

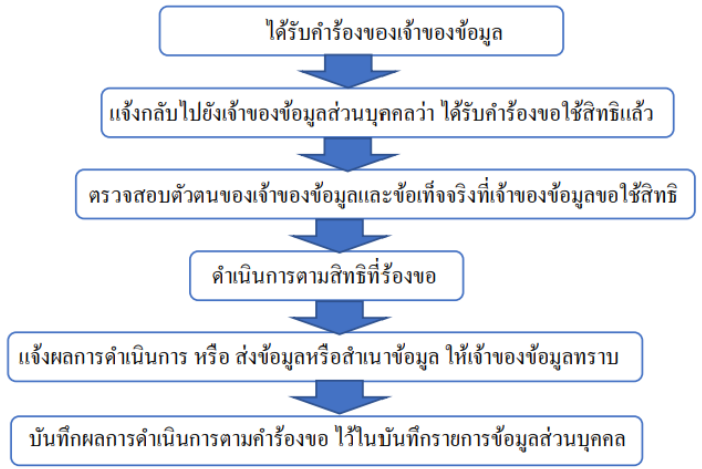
เมื่อท่านแจ้งความประสงค์จะใช้สิทธิของเจ้าของข้อมูลผ่านการกรอกข้อมูลและส่งแบบฟอร์มนี้ บริษัทซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลของท่าน จะแจ้งให้ท่านทราบทาง E-mail เกี่ยวกับการยืนยันว่า บริษัทฯได้รับเรื่องการขอใช้สิทธิของท่านเรียบร้อยแล้ว และแจ้งถึงผลกระทบที่อาจเกิดขึ้น หากผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำร้องขอของท่าน หลังจากนั้น บริษัทฯซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการตรวจสอบคำร้องขอ และพิจารณาว่าสามารถดำเนินการได้หรือไม่ ซึ่งจะได้ดำเนินการและแจ้งผลการตรวจสอบคำร้องของท่านต่อไป

- **ผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล** จากการดำเนินการขอเพิกถอนความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล หรือ การขอให้ลบ ทำลาย ข้อมูลส่วนบุคคล อาจมีดังต่อไปนี้
  - ท่านถอนความยินยอมในการให้เก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ได้เฉพาะข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคล มิได้เก็บ รวบรวม ใช้ ประมวลผล และเปิดเผย เพื่อวัตถุประสงค์ที่บริษัทฯต้องดำเนินการเพื่อปฏิบัติตามกฎหมายเท่านั้น
  - ท่านอาจไม่ได้รับสิทธิประโยชน์ ข่าวสาร ประชาสัมพันธ์ เชิญชวนเข้าร่วมกิจกรรม รับทราบข้อมูลเกี่ยวกับธุรกิจ เสนอสิทธิหรือประโยชน์หรือโอกาสในการใช้บริการ ได้รับสิทธิหรือสิ่งของสมนาคุณ ที่ผู้ควบคุมข้อมูลส่วนบุคคลจัดหาให้แก่ลูกค้า
  - ท่านอาจไม่ได้ข้อเสนอเกี่ยวกับ บริการหรือผลิตภัณฑ์ใหม่ๆของผู้ควบคุมข้อมูลส่วนบุคคล
  - ผู้ควบคุมข้อมูลส่วนบุคคล อาจไม่ทราบถึงความคิดเห็นเพื่อปรับปรุงพัฒนา การบริการและผลิตภัณฑ์จากท่าน ทำให้ไม่สามารถให้บริการหรือนำเสนอผลิตภัณฑ์ที่เหมาะสมกับท่านได้
  - ผู้ควบคุมข้อมูลส่วนบุคคล อาจไม่สามารถดำเนินการอื่นๆที่เกี่ยวข้องกับวัตถุประสงค์ที่กล่าวมาข้างต้นได้
  - หากท่านประสงค์จะขอข้อมูลส่วนบุคคลและข้อมูลการทำธุรกรรมหรือการใช้บริการซึ่งผูกพันไว้กับข้อมูลส่วนบุคคลที่ท่านได้ขอให้ลบ ทำลาย หรือเพิกถอนความยินยอมไปแล้วนั้น ในภายหลัง เพื่อใช้เป็นพยานหลักฐานประกอบการฟ้องร้องคดีหรือเรียกร้องสิทธิตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลที่ดำเนินการตามคำร้องขอ

ตัวอย่างการแบบขอถอนความยินยอม (ต่อ)

ของท่านแล้ว ย่อมไม่อาจให้ข้อมูลดังกล่าวแก่ท่านได้อีกต่อไป ท่านอาจจะเกิดความเสียหายในการได้มาซึ่งข้อมูลหรือพยานหลักฐานในการทำธุรกรรมกับผู้ควบคุมข้อมูลส่วนบุคคลได้

- **บริษัทฯอาจคัดค้านการใช้สิทธิของท่านได้** หากข้อมูลส่วนบุคคลที่ท่านขอให้บริษัทฯดำเนินการตามแบบคำขอนี้ เป็นข้อมูลส่วนบุคคลที่บริษัทฯ เก็บ รวบรวม ใช้ หรือเปิดเผย โดยมีวัตถุประสงค์เพื่อ
  - ปฏิบัติตามกฎหมายที่บริษัทฯมีหน้าที่ต้องปฏิบัติตามอย่างเคร่งครัด
  - เป็นการจำเป็น เพื่อให้เกิดสิทธิเรียกร้องตามกฎหมาย หรือเป็นการปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย หรือยกขึ้นเพื่อต่อสู้สิทธิเรียกร้อง
- เมื่อบริษัทฯได้รับคำร้องขอนี้ บริษัทฯจะดำเนินการดังต่อไปนี้ ภายในระยะเวลาที่แจ้งไว้ข้างต้น



หมายเหตุ : ระหว่างขั้นตอนการตรวจสอบตัวตนของเจ้าของข้อมูลส่วนบุคคลผู้ใช้สิทธิ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจติดต่อเพื่อสอบถามข้อมูลเพิ่มเติมกับผู้ใช้สิทธิ ดังนั้น โปรดให้ข้อมูลการติดต่อที่ถูกต้องด้วย

ส่วนที่ 4 การเลือกใช้สิทธิ

สิทธิที่ท่านเจ้าของข้อมูลส่วนบุคคลจะขอให้บริษัทผู้ควบคุมข้อมูลดำเนินการ

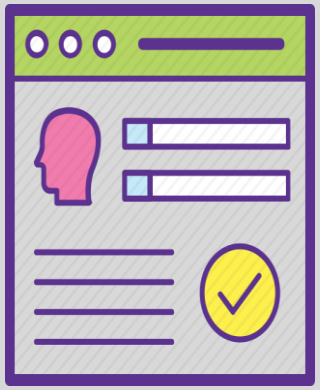
โปรดเลือก	ประเภทสิทธิ	ระยะเวลาดำเนินการ
☐	สิทธิในการขอถอนความยินยอม	7 วัน
☐	สิทธิในการเข้าถึงและขอสำเนาข้อมูล	30 วัน
☐	สิทธิในการขอรับข้อมูลและขอให้ส่งต่อ/โอนข้อมูล	
☐	สิทธิในการคัดค้านการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลของตน	
☐	สิทธิในการขอให้ลบ/ทำลายหรือทำให้ข้อมูลนั้นไม่เป็นข้อมูลส่วนบุคคล	
☐	สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล	
☐	สิทธิในการขอให้ดำเนินการให้ข้อมูลถูกต้องและเป็นปัจจุบัน	
☐	ขอตรวจสอบบันทึกรายการข้อมูลส่วนบุคคล ตามมาตรา 39	

ส่งข้อมูล

หากท่านเจ้าของข้อมูลส่วนบุคคล มีข้อสงสัยหรือต้องการสอบถามข้อมูลเกี่ยวกับการเก็บข้อมูลส่วนบุคคลของบริษัทผู้ควบคุมข้อมูลส่วนบุคคลหรือประสงค์ ท่านสามารถติดต่อสอบถามกับ **"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ DPO (Data Protection Officer)" ตามข้อมูลในเว็ปไซต์ของบริษัทผู้ควบคุมข้อมูลส่วนบุคคลของท่าน** ได้ทันที

Check list การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- นโยบายคุ้มครองข้อมูลส่วนบุคคล สำหรับพันธมิตร คู่ค้า
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับ **Outsourcing**
- นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ประมวลผล **Data Processor**
- นโยบายด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล **(IT Security)**
- แนวทางปฏิบัติ/คู่มือ การละเมิดข้อมูลส่วนบุคคลและการขอใช้สิทธิของเจ้าของข้อมูล



- แบบขอความยินยอม เก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล **(Hard Copy)**
- แบบขอความยินยอม เก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ผ่านเวปไซต์/แอปพลิเคชั่น **(e-Consent)**
- แบบขอเพิกถอนความยินยอมในการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล
- แบบขอใช้สิทธิต่างๆของเจ้าของข้อมูลส่วนบุคคล
- แบบแจ้งการละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

Check list การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- มีการกำหนด/แต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กร
- แจ้งข้อมูล ชื่อ ข้อมูลการติดต่อ สำนักงาน/สถานที่ปฏิบัติงาน ของ DPO ต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล และ เจ้าของข้อมูลส่วนบุคคล
- ให้ความคุ้มครองเจ้าหน้าที่ DPO ขององค์กรตามกฎหมาย

- ประเมินความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลเป็นประจำทุกปี
- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบ IT เป็นประจำทุกปี
- กำหนดมาตรการบรรเทาความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลและด้าน IT และถือปฏิบัติอย่างเคร่งครัด

ข้อพิจารณาในการใช้กฎหมาย PDPA กรณีใช้ Outsourcing

องค์กร

IT Outsource

HR Outsource

House Keeping Outsource

เก็บข้อมูลในนามของใคร

เก็บไปแล้ว ใครเป็นผู้ใช้ข้อมูลเหล่านั้น ?

ข้อมูลที่เก็บ ส่งไปให้ใครเก็บหรือใช้ต่อบ้าง

การตีความ “ผู้รับผิดชอบเรื่อง Data Breach” กรณีใช้ Outsourcing

องค์กร

Outsources

เมื่อข้อมูลส่วนบุคคลรั่วไหล หรือ เกิดการละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล = ผู้เก็บข้อมูลที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล

ผู้ควบคุมข้อมูลส่วนบุคคล = ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล = ผู้ควบคุมข้อมูลส่วนบุคคล

แนวทางการทำข้อตกลง กรณีใช้ Outsourcing

องค์กร

สัญญา

ข้อตกลง

Outsourcing

- นโยบายการคุ้มครองข้อมูลส่วนบุคคลกับคู่ค้า
- ข้อตกลง กำหนดสถานะทางกฎหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ข้อกำหนดเรื่อง มาตรฐานความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

Contact us

บจก. กฎหมายและธุรกิจ อินเตอร์ คอนซัลแตนท์
Inter Consultants Law & Business Ltd.

www.interco.co.th

บริษัท กฎหมายและธุรกิจ
อินเตอร์ คอนซัลแตนท์
จำกัด
399/48 ซอยทองหล่อ 21,
ถนนสุขุมวิท 55 , วัฒนา, กทม
10110

โทร : 02-185-1895 , 02-712-8205
แฟกซ์ : 02-185-1899
Email : interco@interco.co.th

กรณีข้อกฎหมายและแนวทางการปรึกษากฎหมาย

ดร.ญาดา กาศยปนันทน์ (PDPA Advisor)

Inter Consultants Law and Business Ltd.

โทร. 081-987-0138

กรณีงานด้านการเสนอราคาและประสานงาน

คุณชุติมา

Inter Consultants Law and Business Ltd.

โทร. 02-185-1895


THANK
YOU