กฎหมายคุ้มครองข้อมูลส่วนบุคคล

PDPA
STEP BY STEP
ทีละขั้นทีละตอน

8 ขั้นตอนกับการทำ Implement pdpa
แบบเข้าใจง่าย ทำตามได้ไม่ยาก

ดร.ชัชวาล อรวงศ์ศุภทัต
ทนายฝ้าย ยิ่งพร อินทร์ศรีชื่น

PDPA

ทีละขั้นทีละตอน

Implement PDPA Step by Step

ชัชวาล อรวงศ์ศุภทัต
ยิ่งพร อินทร์ศรีชื่น

PDPA ทีละขั้นทีละตอน
Implement PDPA Step by Step

ข้อมูลทางบรรณานุกรม

ชัชวาล อรวงศ์ศุภทัต
ยิ่งพร อินทร์ศรีชื่น
PDPA ทีละขั้นทีละตอน
Implement PDPA Step by Step –
กรุงเทพฯ : นายทำถูก, 2564

ISBN : 978-616-586-415-2

บรรณาธิการ : ชัชวาล อรวงศ์ศุภทัต
ยิ่งพร อินทร์ศรีชื่น

จัดพิมพ์โดย : ชัชวาล อรวงศ์ศุภทัต
ยิ่งพร อินทร์ศรีชื่น

ออกแบบปกโดย : ยิ่งพร อินทร์ศรีชื่น

รูปเล่ม : ยิ่งพร อินทร์ศรีชื่น

พิสูจน์อักษร : สุราสินี ถึงแสง และ
ยิ่งพร อินทร์ศรีชื่น

พิมพ์ที่ : โรงพิมพ์ บริษัท นายทำถูก จำกัด

ความนำ
Implement PDPA Step by Step

จากที่ได้วางขายหนังสือ 108-1009 ถาม-ตอบ PDPA เล่มที่ 1 รวม 50 คำถาม-ตอบที่เราได้รับบ่อย ๆ มาประมวลตอบ และหนังสือ PDPA for HR ซึ่งก็นับเป็นหนังสือ PDPA ภาคปฏิบัติเล่มที่ 2 ของเราไปแล้ว พบว่า ได้รับการตอบรับจากท่านผู้อ่านในระดับที่น่าพึงพอใจเลยทีเดียว เราก็เลยได้จัดทำเล่มที่ 3 ต่อเนื่องกัน แต่ไม่ได้ทำออกมาในลักษณะของการถาม-ตอบเช่นสองเล่มก่อน หากจะเน้นการให้คำแนะนำในการ Implement PDPA ในองค์กรแบบ Step by Step ที่เราเชื่อว่าจะเป็นประโยชน์อย่างมากกับท่านผู้อ่าน ที่จะได้ไอเดียและแนวทางจากเราที่ทำงานทั้งวิทยากรและงานที่ปรึกษาในการ Implement PDPA ในองค์กรหลายแห่งไปปรับใช้

ก่อนหน้าที่จะวางหนังสือเล่มนี้ เราได้จัดทำเวอร์ชั่นพิเศษ ซึ่งได้นำเอาเนื้อหาส่วนหนึ่งของหนังสือเล่มนี้ไปจัดทำ e-book เพื่อระดมทุนสนับสนุนการปฏิบัติงานช่วยผู้ป่วยโควิด-19 ของมูลนิธิสถาบันการวิจัยและนวัตกรรมด้านเอชไอวี (IRHI) ซึ่งมีบุคลากรทำงานช่วยเหลือผู้ป่วยอย่างแข็งขันองค์กรหนึ่งในสังคมไทย และเราก็รู้สึกปลื้มใจที่ได้นำเอาความรู้และประสบการณ์ด้าน PDPA ที่เรามี ไปเป็นสะพานบุญ เพื่อให้ท่านผู้อ่านได้ร่วมกันบริจาค ก็พบว่ามีบางท่านบริจาคเป็นเงินหลายพันบาท บางท่านก็หลายร้อยบาท เกินกว่าที่พวกเราได้คาดหมายไว้ ก็ใคร่ขออนุโมทนาบุญกุศลครั้งนี้กับทุกท่านที่ร่วมบริจาคมา และเราก็เชื่อว่า เนื้อหาที่ได้เรียบเรียงออกไปจะเป็นประโยชน์กับทุกท่านที่ร่วมทำบุญดังกล่าวเป็นอย่างมาก

หนังสือเล่มนี้ มีเนื้อหาที่ละเอียดมากกว่าเล่ม e-book ที่เราทำเพื่อการกุศลอย่างมาก อธิบายขยายความลงรายละเอียดมากขึ้น มีหัวข้อให้เรียนรู้ มีตัวอย่างของเอกสารและแบบฟอร์มในหลากหลายเรื่องมากขึ้น ตัวอย่างของหัวข้อที่เราได้จัดทำเพิ่มขึ้นได้แก่ กิจกรรมและองค์กรที่ไม่ต้องปฏิบัติตามกฎหมาย PDPA หลักการเก็บรวบรวมข้อมูลส่วนบุคคล หลักการใช้และเปิดเผยข้อมูลส่วนบุคคล การส่งและโอนข้อมูลส่วนบุคคลไปต่างประเทศ เป็นต้น

ความนำ
Implement PDPA Step by Step

กับเรื่องที่สำคัญมากในเล่มนี้ ที่ท่านพลาดไม่ได้เลยก็คือ ตัวอย่างของการปรับปรุงแก้ไขขั้นตอนหรือวิธีการปฏิบัติงาน เพื่อให้สอดคล้องกับกฎหมาย PDPA อย่างไรก็ตาม ตัวอย่างก็เป็นเพียงอย่างย่อเท่านั้น ยากที่จะเขียนให้เห็นภาพละเอียดลออได้ในทุกแง่มุม แต่ก็เชื่อมั่นว่า จะช่วยให้ท่านได้เห็นภาพความเป็นจริงในการทำงานให้สอดคล้องกับกฎหมาย PDPA ได้ว่า ในกระบวนการของการปรับปรุงแก้ไขขั้นตอนในวิธีการปฏิบัติงาน ซึ่งเป็นขั้นตอนที่ 7 ใน 8 ขั้นตอนที่เราแนะนำในการทำ Comply PDPA นี่ละ เป็นส่วนที่ยากและเยอะ และก็เป็นเรื่องหลักที่จะทำให้องค์กรของท่านไม่พลาดในการทำงานให้สอดคล้องกับกฎหมาย PDPA และเราก็ได้พยายามอธิบายออกมาให้ท่านได้เห็นภาพและเข้าใจง่าย ๆ เท่าที่เราจะสามารถทำได้

และต้องบอกไว้ด้วยเช่นกันว่าหนังสือ PDPA ของเรา เล่มที่ท่านถืออยู่ในมือนี้ เป็นเล่มที่ 3 แล้ว และเราก็คาดว่าจะทำหนังสือออกมาให้เล่มนี้เป็นเล่มสุดท้ายในเรื่อง PDPA โดยสองเล่มก่อนหน้าจะเน้นการเขียนแบบถาม-ตอบ ทั้งในเรื่อง PDPA ทั่วไป (เล่มที่ 1) และถาม-ตอบในเรื่อง PDPA ในงาน HR (เล่มที่ 2) และแนวทางการเขียนหนังสือเล่มนี้ก็ไม่ได้เป็นแบบถามตอบทั้งเล่ม คงมีแนวการถามตอบแทรกในบางเรื่องเท่านั้น โดยได้พยายามอธิบายหลักการที่เกี่ยวข้อง เพื่อให้ท่านได้เข้าใจว่าที่มาที่ไปของเรื่องราวนั้นเป็นอย่างไร แต่ก็แน่นอนว่า เราไม่ได้เขียนเป็นตำราแต่อย่างใด และก็ไม่ได้ย้อนเท้าความไปพูดถึงประวัติที่มาของกฎหมายให้มากความไป เพราะเราไม่ต้องการให้ท่านรู้สึกว่า PDPA มันเป็นเรื่องยากเหลือหลาย จากความจริงที่มันก็ไม่ง่ายเช่นกัน

ด้วยความเชื่อมั่นว่าท่านจะได้นำสิ่งที่ได้เรียนรู้จากเราไปใช้ประโยชน์

ดร.ชัชวาล อรวงศ์ศุภทัต
ทนายความ ยิ่งพร อินทร์ศรีชื่น
กันยายน 2564

ความนำ
Implement PDPA Step by Step

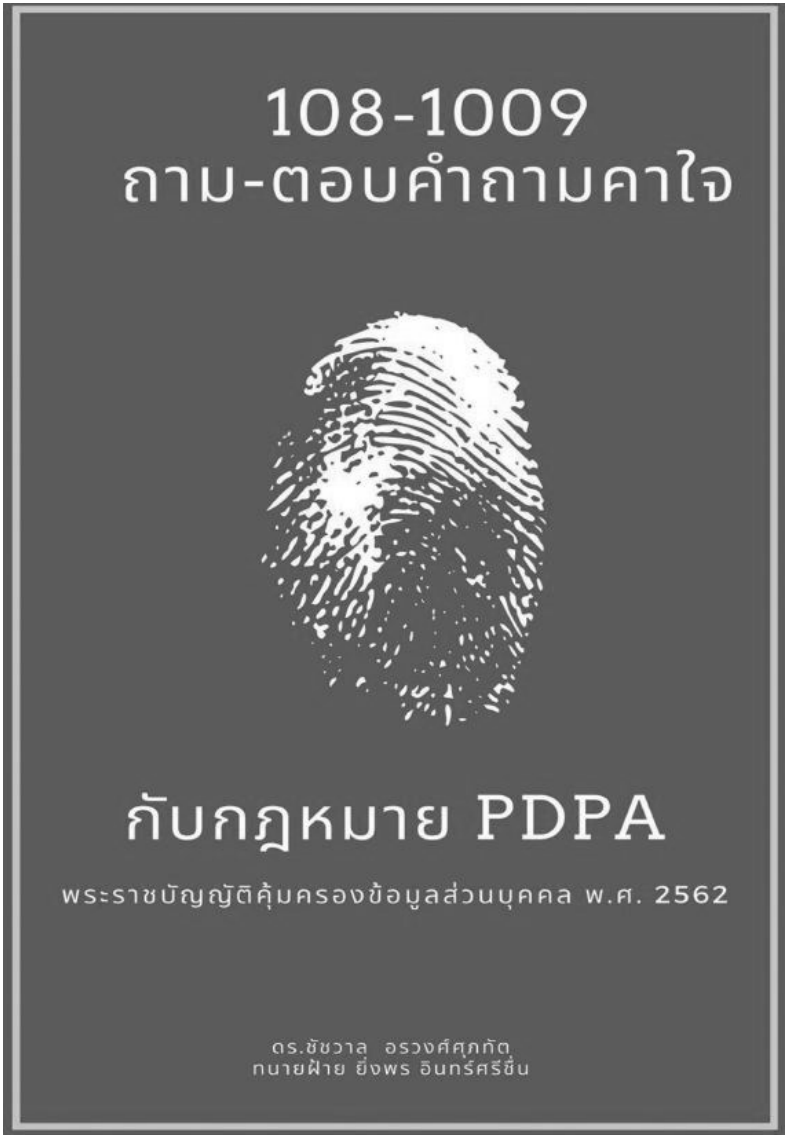
ทบทวนเรื่อง PDPA

ดร.ชัชวาล อรวงศ์ศุภทัต และทนายความ ยิ่งพร อินทร์ศรีชื่น

สารบัญ
Implement PDPA Step by Step

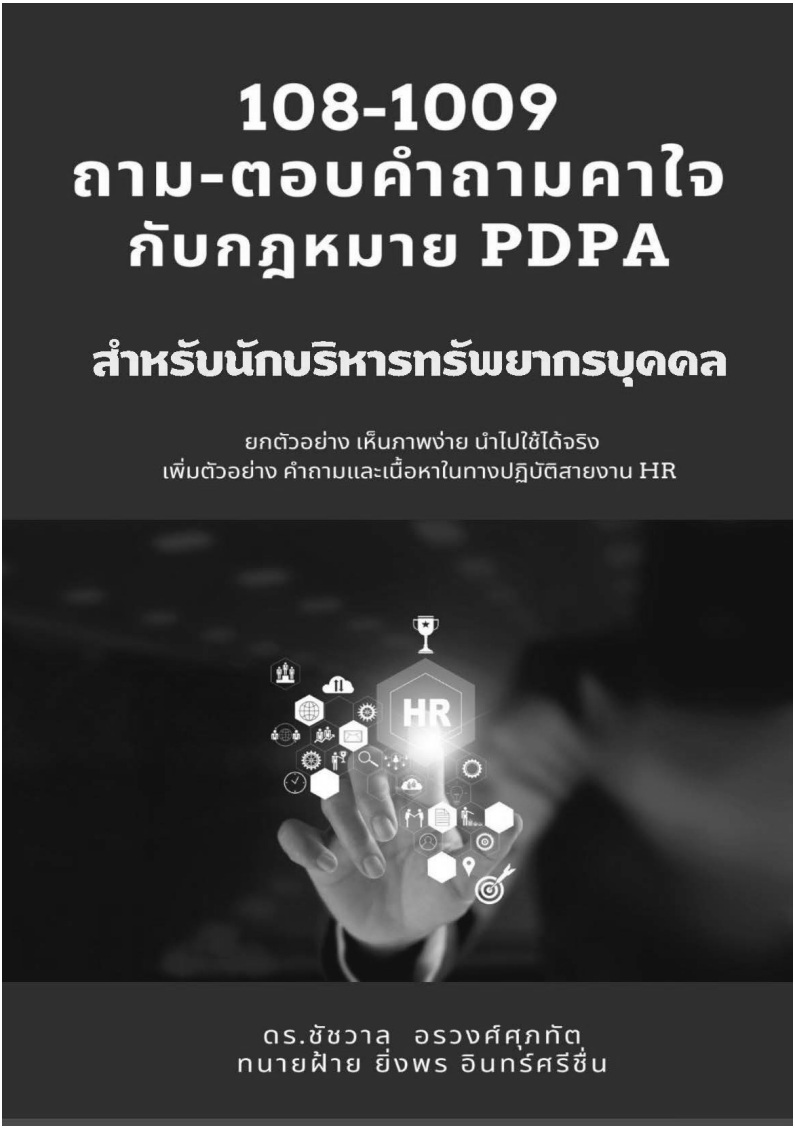
สารบัญ (ต่อ)
Implement PDPA Step by Step

แนะนำหนังสือของเรา
(เล่ม 1) 50 คำถาม-ตอบ PDPA



ดร.ชัชวาล อรวงศ์ศุภทัต และทนายความ ยิ่งพร อินทร์ศรีชื่น

แนะนำหนังสือของเรา
(เล่ม 2) PDPA for HR



ดร.ชัชวาล อรวงศ์ศุภทัต และทนายความ ยิ่งพร อินทร์ศรีชื่น

ทบทวนเรื่อง PDPA

PDPA in General

ดร.ชัชวาล อรวงศ์ศุภทัต และทนายความ ยิ่งพร อินทร์ศรีชื่น

1 กฎหมาย PDPA คืออะไร ?

กฎหมาย PDPA หรือที่เราเรียกกันสั้น ๆ ว่า PDPA นั้น ก็คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือในภาษาอังกฤษก็จะเรียกว่า Personal Data Protection Act นั้น ตราขึ้นมาตั้งแต่ปี พ.ศ.2562 ที่ผ่านมา กฎหมายนี้ มีขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก และมาตรการในการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ในอันที่จะห้ามเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือไม่มีอำนาจที่กฎหมายบัญญัติเอาไว้ให้สามารถดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้โดยไม่ต้องขอความยินยอม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมาย PDPA นี้ อันที่จริงไม่ได้บังคับใช้กับทุกองค์กร และผู้ควบคุมข้อมูลส่วนบุคคลจำนวนหนึ่งที่ไม่ต้องบังคับตามกฎหมาย ซึ่งกำหนดไว้เรียบร้อยในมาตรา 4 อันได้แก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจ

ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลลำดับที่ (2) - (6) แม้จะไม่ต้องว่ากันตามกฎหมายนี้ ก็จะต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย เพียงแต่มาตรฐานของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น จะเป็นอย่างไร ก็ต้องไปว่ากันในรายละเอียดอีกที

2 กฎหมาย PDPA สำคัญกับองค์กรอย่างไร ?

หากพิจารณากันว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมาย PDPA นี้สำคัญกับองค์กรอย่างไร เห็นทีต้องคุยกันในมุมของประโยชน์ที่องค์กรจะได้รับจากการปฏิบัติหรือดำเนินการตามกฎหมายที่ว่านี้ ซึ่งผู้รู้ท่านก็แนะนำไว้ในทำนองที่สอดคล้องกัน เช่น

(1) การมีกฎหมายนี้ย่อมช่วยเพิ่มความเชื่อมั่นในมาตรฐานของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อคู่ค้า ลูกค้า หรือพันธมิตรในการดำเนินงานขององค์กรไม่ว่าจะในประดับประเทศหรือระดับนานาชาติ หากเป็นองค์กรภาคธุรกิจเอกชนที่ดำเนินธุรกิจในต่างประเทศที่เค้าบังคับใช้กฎหมายลักษณะนี้ด้วยแล้ว ก็ย่อมที่จะเป็นตัวช่วยสร้างความเชื่อมั่นในการค้าขายระหว่างกันในทางหนึ่ง และที่ว่าไปนี้ หากจะกล่าวว่าเป็นการเพิ่มขีดความสามารถในการแข่งขันขององค์กรก็ไม่ผิดนัก

(2) กฎหมาย PDPA ช่วยให้องค์กรได้ทบทวนกระบวนการดำเนินงานหรือขั้นตอนการปฏิบัติ เนื่องจากจะต้องมาปรับเปลี่ยนเพื่อให้ขั้นตอนการปฏิบัติงานใดใดนั้นไม่ขัดหรือแย้งกฎหมาย หากองค์กรใดไม่ได้จัดทำขึ้นตอนการปฏิบัติงานไว้ ก็ถือเป็นโอกาสที่ดีที่จะได้จัดทำขึ้น และออกแบบให้สอดคล้องกับกฎหมาย PDPA นี้ให้เรียบร้อย ในทำนองหนึ่ง องค์กรก็จะได้ทบทวนด้วยว่า ขั้นตอนการปฏิบัติงานหนึ่งใดนั้น มันมีความซ้ำซ้อนหรือไม่กระชับไม่รัดกุมในเรื่องใดบ้าง ก็จะได้ปรับแก้ก่อนที่จะไปจัดการให้สอดคล้องกับกฎหมาย PDPA ในท้ายที่สุด

(3) เป็นที่น่าเชื่อถือและเสริมภาพลักษณ์การเป็นผู้ประกอบการหรือองค์การที่ให้บริการสาธารณะที่คุ้มครองความเป็นส่วนตัวของลูกค้าหรือผู้รับบริการ ซึ่งย่อมเป็นเรื่องที่ดีแน่ โดยเฉพาะการส่งเสริมภาพลักษณ์ของการเป็นองค์กรที่มีธรรมาภิบาลนี้ ถือเป็นเรื่องใหญ่ที่ไม่ว่าองค์กรภาครัฐ รัฐวิสาหกิจ หรือภาคเอกชนต่างตื่นตัวกันอย่างมากในรอบหลายปีที่ผ่านมา

อันที่จริง กฎหมาย PDPA นี้ ยังสำคัญหรือมีประโยชน์แก่ตัวพนักงานของบุคลากรขององค์กร ในฐานะที่ก็เป็นเจ้าของข้อมูลด้วย อย่างน้อยที่สุดในฐานะของเจ้าของข้อมูลส่วนบุคคล ก็จะได้มั่นใจว่าข้อมูลส่วนบุคคลของตนเองจะได้รับการจัดเก็บอย่างปลอดภัย เหมาะสมและจะถูกนำไปใช้ เผยแพร่ตามวัตถุประสงค์ที่ตนเองได้บอกหรือได้แจ้งไว้กับผู้ประกอบการ ก็สบายใจหายห่วงไป

และหากมีการละเมิดข้อมูลส่วนบุคคล ก็จะได้รับการเยียวยาความเสียหายที่เกิดจากการละเมิดนั้น ซึ่งหากไม่มีกฎหมายนี้ คงยากที่บุคคลธรรมดาสามัญจะไปเอาเรื่องเอาราวผู้ประกอบการได้ถนัดนัก แต่ภายใต้กฎหมายนี้ เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เสียหาย สามารถร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้มีการชดใช้ค่าสินไหมทดแทนการละเมิดจากผู้ประกอบการที่ได้ใช้ข้อมูลส่วนบุคคลผิดแผกไปจากวัตถุประสงค์ที่ตนได้ยินยอมหรืออนุญาตไว้ เป็นต้น

นอกเหนือจากนี้ ส่วนที่สำคัญมากอีกอย่างหนึ่งก็คือ กฎหมาย PDPA เองให้การรับรองสิทธิ 8 อย่างของเจ้าของข้อมูลส่วนบุคคล และเป็นหน้าที่ของผู้ประกอบการ (ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล) ที่จะต้องเปิดให้เจ้าของ

เจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิที่พึงมีพึงได้ตามกฎหมาย เช่น สิทธิในการทราบการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของตนเอง สิทธิในการเพิกถอนความยินยอม สิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดเก็บไว้ และยังสามารถขอให้ทำการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่อาจบ่งชี้กลับมาที่ตนที่เป็นเจ้าของข้อมูลส่วนบุคคลก็ได้ นี่เป็นเพียงส่วนหนึ่งของสิทธิ 8 อย่างที่กฎหมายรับรองและคุ้มครองให้

3 กิจกรรมและใครบ้างที่ไม่ต้องปฏิบัติตามกฎหมาย PDPA

ก่อนที่จะไปกล่าวถึงเรื่องของกิจกรรมและใครบ้างที่ไม่ต้องปฏิบัติตามกฎหมาย PDPA นี้ อยากคุยให้ฟังถึงเรื่องขอบเขตของการใช้กฎหมาย PDPA นี้เสียหน่อย ซึ่งต้องไปดูจากมาตรา 3 สรุปอย่างง่าย ๆ ได้ว่า หากบ้านเมืองเรามีกฎหมายใดใดที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะ ก็บังคับได้ตามกฎหมายนั้น เช่น เรามีกฎหมายเกี่ยวกับข้อมูลเครดิต ที่มีบทบังคับในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องราวไว้ ก็ว่ากันไปตามกฎหมายที่ว่านั้น แต่หากกฎหมายอื่นใดไม่ว่าจะมีหรือไม่มีเรื่องเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล และเรื่องบทกำหนดโทษที่เกี่ยวข้อง ก็เอากฎหมาย PDPA นี้ไปใช้บังคับเพิ่มเติมได้ ไม่ว่าจะซ้ำกับกฎหมายอื่นหรือไม่ก็ตาม นอกจากนี้ หากเป็นเรื่องที่เกี่ยวกับการร้องเรียนเรื่องที่คณะกรรมการผู้เชี่ยวชาญตามกฎหมาย PDPA มีอำนาจเฉพาะ เช่นการออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคลเป็นต้น และกฎหมายอื่นใดที่พูดถึงเรื่องการคุ้มครองข้อมูลส่วนบุคคลนั้นไม่มีเรื่องร้องเรียนไว้เฉพาะก็ว่ากันตามกฎหมาย PDPA ได้ หรือกฎหมายอื่นมีเรื่องของการร้องเรียนอยู่ แต่หากยังไม่เพียงพอแก่การคุ้มครองเจ้าของข้อมูลส่วนบุคคล ก็ว่ากันตามกฎหมาย PDPA นั่นเอง

กลับมาที่หัวข้อหลัก ก็ต้องบอกว่า กฎหมาย PDPA ไม่ได้ใช้บังคับกับทุกกิจกรรมหรือกับทุกหน่วยงาน ซึ่งมาตรา 4 ของกฎหมายนี้ ก็เขียนยกเว้นไว้ชัดเจน ประกอบด้วยกรณี

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทาการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอานาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการแล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดีการบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลลำดับ (2) (3) (4) (5) และ (6) รวมทั้งผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กฎหมายจะได้ประกาศกำหนดในอนาคตนั้น ก็มีหน้าที่ตามกฎหมายที่จะต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย แต่มาตรฐานที่ว่านั้น จะเป็นเพียงใดและอย่างไรบ้าง กฎหมายไม่ได้บอกเอาไว้ชัด ๆ

ซึ่งก็คงเป็นเรื่องที่เราเองจะต้องคอยติดตามดูว่าจะเป็นอะไรและอย่างไรต่อไป

อยากจะขยายความไว้ว่าในข้อยกเว้นการไม่ต้องปฏิบัติตามกฎหมาย PDPA ในเรื่องแรกที่เป็นเรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลออกมา เพราะมีคำถามจากผู้เข้ารับการอบรมหรือองค์กรที่เราเป็นที่ปรึกษามาพอสมควรว่าขอบเขตของประโยชน์ส่วนตนหรือกิจกรรมในครอบครัวนั้นมีเพียงใด เรื่องนี้ ต้องไปดูที่แนวของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของทางสหภาพยุโรป หรือที่ท่านทั้งหลายจะคุ้นว่า GDPR (General Data Protection Regulation) ซึ่งบอกไว้ว่าเป็นเรื่องที่ไม่เกี่ยวข้องกับกิจกรรมทางวิชาชีพหรือในการพาณิชย์ (Commercial Activity) เช่น การติดต่อสื่อสารกันทางสื่อออนไลน์กันเป็นการส่วนตัว ในในครอบครัว การถ่ายภาพกิจกรรมส่วนตัว หรือบุคคลในรอบครัว แต่หากเป็นการถ่ายภาพส่วนบุคคลของตนมาเพื่อประโยชน์ทางการค้า เช่นการขายของออนไลน์ แบบนี้ จะเป็นเรื่องทางการค้าหรือการพาณิชย์ทันที ก็ต้องว่ากันไปตามกฎหมาย PDPA และในบางกรณี เช่นเรื่องของการกุศล แม้จะดูเป็นเรื่องส่วนตัวก็ตาม แต่ตามแนวทางของ GDPR ก็ถือว่ากิจกรรมเกี่ยวกับการกุศลนั้น ไม่ได้เป็นเรื่องของประโยชน์ส่วนตนหรือเป็นกิจกรรมเพื่อประโยชน์ของบุคคลในครอบครัวแต่อย่างใด แต่ในประเทศไทยนั้น จะเป็นอย่างไรบ้าง คงต้องคอยติดตามแต่ละกรณีกันต่อไป

ยกตัวอย่างอีกสักเรื่องที่เป็นข้อยกเว้นของการบังคับใช้กฎหมาย PDPA คือเรื่องที่หน่วยงานของรัฐที่มีหน้าที่รักษาความมั่นคงของรัฐนั้น ผู้รู้ท่านแนะไว้ว่า องค์กรภาครัฐที่ปฏิบัติงานตามกฎหมายหลัก 3 ฉบับ อันได้แก่ กฎหมายสภาความมั่นคงแห่งชาติ กฎหมายข่าวกรองแห่งชาติ และกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งตราออกมาในเวลาใกล้เคียงกับกฎหมาย PDPA คือในปี พ.ศ.2562 นี้เอง นี่เป็นอีกตัวอย่างหนึ่ง ซึ่งเราจะไม่ลงรายละเอียดแต่อย่างใด เพราะรายละเอียดนั้น เชื่อว่าท่านผู้อ่านที่อยากทราบ ก็ย่อมไปศึกษาค้นคว้าเชิงลึกได้ตามตำราที่เขียนเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างไม่ยากเย็นนัก

เรามาลองยกตัวอย่างในเรื่องที่ว่าไปเมื่อสักครู่ให้เห็นภาพกัน ถามว่า เจ้าหน้าที่ตำรวจจราจร จัดให้มีการถ่ายภาพหรือบันทึกภาพ

รถยนต์ที่คนขับขับขี่ผิดกฎจราจรไว้ มีการเก็บรวบรวมข้อมูลทะเบียนรถ ซึ่งสามารถเชื่อมโยงไปถึงตัวของเจ้าของรถ เช่น บัตรประชาชน ใขอนุญาตขับขี่ หรือหลักฐานทางทะเบียนรถ เป็นต้น นี่ก็นับเป็นการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลอย่างแน่นอน แถมยังมีหลายเรียกให้ไปชำระค่าปรับจากการผิดกฎจราจรอีกต่างหาก แบบนี้ เป็นการปฏิบัติงานหรือดำเนินงานของหน่วยงานภาครัฐที่มีหน้าที่รักษาความมั่นคงปลอดภัยของประชาชนหรือไม่

คำตอบคือ “เป็น” จึงเข้าข่ายมาตรา 4 (3) ซึ่งก็ไม่ต้องปฏิบัติตามกฎหมาย PDPA นั่นเอง แม้ว่าดูแล้วหน่วยงานจะมีลักษณะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามความหมายของกฎหมาย PDPA แต่ก็ไม่ต้องว่ากันตามกฎหมายนี้แต่อย่างใด และแน่นอนที่ว่า เจ้าของข้อมูลส่วนบุคคลคือผู้ขับขี่ หรือเจ้าของรถก็ไม่สามารถใช้สิทธิของตนในฐานะที่เป็นเจ้าของข้อมูลส่วนบุคคลได้เลย

อีกเรื่องหนึ่งที่หากจะไม่พูดไว้ก็จะเป็นการไม่ครบถ้วน ก็คือขอบเขตเชิงพื้นที่ของการบังคับใช้กฎหมาย PDPA

อันนี้ต้องไปดูที่มาตรา 5 ว่าไว้ โดยสรุปก็จะได้ว่า กฎหมาย PDPA นี้ ใช้บังคับกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม และก็อย่าลืมว่า ราชอาณาจักรนั้น ไม่ได้หมายถึงพื้นที่ประเทศไทย 77 จังหวัดเท่านั้นนะ เพราะตามกฎหมายแล้ว มีพื้นที่บางอย่าง แม้จะอยู่ต่างประเทศ ก็ถือว่าเป็นราชอาณาจักรไทย ยกตัวอย่างเช่น มีคนกระทำความผิดอาญาในเรือหรืออากาศยานไทย กฎหมายอาญา (ไม่ใช่ตัวกฎหมาย PDPA) ก็ถือว่าเป็นการกระทำความผิดในราชอาณาจักรไทยด้วย

หากเจาะลงไปที่กิจกรรมแล้ว หากเป็นกิจกรรมที่ (1) เป็นการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม หรือ (2) มีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรไทยแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ต้องปฏิบัติตามกฎหมาย PDPA

ดังนั้น หากบริษัท ABC จัดตั้งในประเทศไทย ทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลลูกค้าที่เป็นคนไทย แม้ลูกค้าจะไม่ได้มีสัญชาติไทยก็ตาม บริษัท ABC ก็ต้องทำตามกฎหมาย PDPA หรือบริษัท XYZ จัดตั้งในประเทศไทย แต่มี Server เก็บข้อมูลลูกค้าของตนเองอยู่ในต่างประเทศ หรือบริษัท XYZ นั้น ส่งข้อมูลส่วนบุคคลของลูกค้าไปประมวลผลที่ต่างประเทศ ก็ต้องทำตามกฎหมาย PDPA เช่นกัน

4 หากไม่ทำ PDPA องค์กรจะมีปัญหาอะไรหรือไม่นะ ?

มีประเด็นถามไถ่เรื่องนี้กันเสมอ จากผู้บริหาร และพนักงานในหลายองค์กรว่าหากไม่ทำตามกฎหมาย PDPA แล้วจะมีความผิดอะไรหรือเปล่า หรือบางครั้งตัวผู้ประกอบการเองก็ถามโพล่ง ๆ ออกมาเลยว่า ทำ PDPA ไปแล้ว หรือหากไม่ทำแล้วทางองค์กรภาครัฐที่เป็น Regulator คือทางสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเขาจะมาตราวจสอบหรือว่าองค์กร Comply กับกฎหมาย PDPA หรือไม่ เค้าคงไม่มีอัตรากำลังคนมาตราวจสอบหรอก ไม่เห็นจะต้องทำให้เสียเงินและเสียเวลาเลย

ขอคุยเรื่องนี้เสียหน่อยว่า อันที่จริง ท่านไม่ต้องกังวลว่าทาง Regulator หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเขาจะมาตราวจสอบหรอก ขอให้ท่านกังวลว่าการทำผิดกฎหมายมันก็คือผิด เพียงแต่เรื่องยังไม่แดงขึ้นมา เท่านั้น แต่ขอให้กังวลว่าทางเจ้าของข้อมูลส่วนบุคคลเขาจะไปร้องเรียนกับหน่วยงานที่เกี่ยวข้องเอา เมื่อนั้นจะลำบากเลย ลองดูจากเคสของ GDPR หรือการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศทางสหภาพยุโรปดูท่านก็จะเห็นว่า ที่องค์กรหรือผู้ประกอบการโดนปรับนั้นส่วนมากแล้วไม่ได้มาจากทาง Regulator เค้ามาตราวจหรอกนะ แต่เกิดจากเจ้าของข้อมูลส่วนบุคคลนี่ล่ะเค้าไปฟ้องร้อง หรือไปร้องเรียนกับหน่วยงานที่เกี่ยวข้อง จึงขอให้ระวังเรื่องแบบนี้ ดีกว่าที่จะไปกังวลว่า Regulator เขาจะมาตราวจสอบว่าเรา Comply กับกฎหมาย PDPA หรือไม่ เพราะหากมีเรื่องร้องเรียนเกิดขึ้น ก็จะมีการมาตราวจสอบเชิงลึกกันแน่ ๆ

กลับไปประเด็นที่ว่า แล้วไม่ทำตามกฎหมาย PDPA จะเกิดอะไรขึ้น ตอบกันง่าย ๆ ตรงนี้เลยว่าก็ผิดกฎหมาย PDPA นั่นเอง และตัวกฎหมายนี้ก็มีโทษสามแบบเลย ทั้งโทษอาญา (ปรับและจำคุก) โทษปรับทางปกครอง และโทษหรือความรับผิดทางแพ่งจากการทำให้บุคคลอื่นได้รับความเสียหายทางละเมิด ที่สำคัญนั้นอยากให้ดูมาตรา 81 ซึ่งสรุปความจากตัวบทกฎหมายได้ว่า หากผู้กระทำผิดกฎหมายนี้เป็นนิติบุคคล (ก็คือบริษัท หรือองค์กรภาครัฐที่ต้องปฏิบัติตามกฎหมายทั้งหลายนั่นล่ะ) อันเป็นการกระทำผิดที่เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลนั้นมีหน้าที่ต้องสั่งการ หรือกระทำการ หรือละเว้นไม่สั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ผู้นำ ซึ่งก็หมายถึงกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ต้องรับโทษตามที่บัญญัติสำหรับความผิดนั้น ๆ ด้วย โดยเฉพาะหากความผิดตามกฎหมาย PDPA นั้นมีโทษจำคุก บุคคลที่เป็นกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล ก็อาจจะต้องรับโทษจำคุกด้วย

หรือในกรณีที่บุคคลนั้นมีหน้าที่ต้องสั่งการ หรือกระทำการหรือละเว้นไม่สั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ผู้นำ ซึ่งก็หมายถึงกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ต้องรับโทษตามที่บัญญัติสำหรับความผิดนั้น ๆ ด้วย โดยเฉพาะหากความผิดตามกฎหมาย PDPA นั้นมีโทษจำคุก บุคคลที่เป็นกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล ก็อาจจะต้องรับโทษจำคุกด้วย

เพราะจำคุกนิติบุคคลไม่ได้ ก็ต้องจำคุกเอากับกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนี่ล่ะ

ถ้าแบบนี้ ก็ระมัดระวังกันเสียหน่อย จะเอาหูไปนา เอาตาไปไร่ ไม่ใส่ใจสนใจกฎหมาย PDPA แล้วหากเกิดปัญหาการละเมิดข้อมูลส่วนบุคคลของใครก็ตาม ไม่ว่าจะเป็นลูกค้า พนักงาน ผู้สมัครงาน ก็อาจจะเคลียร์ไม่ไหว ตั้งรับไม่ทันสถานการณ์ก็ได้ เราแนะนำว่าอย่าประมาทไป เดี๋ยวจะเข้าทำนองเสียน้อยเสียยาก เสียมากเสียง่าย และบานปลายไปถึงเรื่องการเสื่อมเสียภาพลักษณ์ขององค์กร ซึ่งก็

ต้องยอมรับกันว่า กว่าจะสร้างภาพลักษณ์องค์กรให้ดีงามได้มาจนถึงวันนี้ มันไม่ง่ายและใช้งบประมาณไปก็น่าจะไม่น้อย แต่อาจจะต้องมาเสียไปแบบง่าย ๆ เพียงเพราะอารมณ์ประมาณว่า เสียเวลา

ยิ่งกับผู้บริหารมืออาชีพที่องค์กรเค้าว่าจ้างมาทำงาน ย่อมเป็นที่คาดหมายว่าจะต้องไม่ทำผิดกฎหมายเสียเอง แต่ด้วยความบางท่านก็คิดแต่ว่าเสียเวลาทำมาหารายได้ ทำตามกฎหมาย PDPA มีแต่เสียเงิน หากเกิดเรื่องราวละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมา ก็อาจจะถูกเล่นงานหนักจากผู้ถือหุ้นที่เป็นเจ้าขององค์กรตัวจริงเอาได้ น่าเสียดายความเป็นนักบริหารมืออาชีพแต่ต้องมาตกม้าตายกับเรื่องที่ไม่ทำตามกฎหมาย PDPA นี้

ผู้ประกอบการหลายท่านไม่ได้สนใจกฎหมาย PDPA เพราะเคยมีประสบการณ์กับกฎหมายความปลอดภัยมาแล้วพบว่าไม่มีใครมาตราจสอบว่าองค์กรได้ทำเรื่องความปลอดภัย อาชีวอนามัยและสภาพแวดล้อมในการทำงานหรือไม่ เพียงใดก็เลยชะล่าใจ เพราะลำพังพนักงานไม่มีใครไปร้องเรียนอยู่แล้ว แต่กับกฎหมาย PDPA เจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มีแต่พนักงานอย่างเดียว ยังมีลูกค้า คู่ค้า และผู้สมัครงานอีกด้วย เราจะทำงานแบบ “วัดใจ” กับบุคคลเหล่านี้หรือไม่ว่าเขาจะไม่ไปร้องเรียนการกระทำผิดกฎหมาย PDPA ขององค์กรของเรา

เมื่อมีปัญหาเช่น ข้อมูลส่วนบุคคลอ่อนไหวของลูกค้ารั่วไหลไป และมีเรื่องร้องเรียนขึ้นมา ฟ้องร้องกันตามติดต่อเนื่อง ก็อย่าโวยวายไปเอาเรื่องไปราวกับพนักงานล่ะ เพราะตอนที่พนักงานบอกให้ผู้ประกอบการทำ ผู้ประกอบการบอกว่าเปลืองเงินเปลืองทองไม่อยากทำ

สำหรับพนักงาน ที่จะต้องระมัดระวังการปฏิบัติตามกฎหมายนั้นก็อยากจะบอกว่า แม้พนักงานมีฐานะเป็นผู้ทำการแทนผู้ควบคุมข้อมูลส่วนบุคคล ก็ไม่ใช่ว่านึกอยากจะทำอะไรก็ทำ หรือไม่สนใจใยดีที่จะปฏิบัติตามกฎหมาย หรือปล่อยปละละเลยไม่ดูแลรักษาข้อมูลส่วนบุคคลที่ตนเกี่ยวข้อง จนเกิดปัญหาข้อมูลรั่วไหลแล้วเกิดความเสียหายกับเจ้าของข้อมูลส่วนบุคคล หากเกิดสถานการณ์เช่นนั้นขึ้น ท่านคิดว่าเจ้าของข้อมูลส่วนบุคคลที่เขาเดือดร้อน นอกจากเขาจะร้องเรียนหรือฟ้องร้ององค์กรแล้ว เขาจะพ่วงฟ้องร้องผู้ปฏิบัติงานเข้าไปด้วยหรือไม่

ฟันธงชัวร์ ๆ ได้ว่าฟ้องพ่วงเข้าไปแน่นอน และถึงจุดนั้น เดิมที่เป็นอยู่ว่า องค์กรหรือผู้บริหารระดับสูง ไม่ค่อยสนใจที่จะปฏิบัติตามกฎหมาย PDPA เมื่อจะถูกปรับสัก 3 ล้านบาท เพราะทำผิดกฎหมาย

PDPA ท่านคิดว่าบริษัททั้งหลาย เขาจะส่งทนายความไปให้การว่า เขาสนใจหรือไม่สนใจที่จะปฏิบัติตามกฎหมายล่ะ เรื่องแบบนี้ ทายกันได้ไม่ยากโดยไม่ต้องพึ่งพ่อหมอหรือแม่หมอคนใดมาฟันธงแต่อย่างใดเลย

แล้วก็เป็นไปได้มากเลยที่หวยจะออกที่ท่าน เพราะองค์กรก็อาจจะบอกว่า ท่านไม่ปฏิบัติตามระเบียบหรือกฎกติกาตามที่องค์กรออกไว้ตามกฎหมาย กลายเป็นงานเข้าตัวท่านเอง แม้องค์กรในฐานะนายจ้างจะช่วยจ่ายค่าสินไหมทดแทนนั้นให้กับผู้เสียหาย ท่านคิดว่า องค์กรจะไล่เบี้ยเอากับท่าน หรือเปล่าล่ะ ทั้ง ๆ ที่อันที่จริง องค์กรเองนั่นล่ะไม่สนใจที่จะทำตามกฎหมาย

อุทาหรณ์เรื่องนี้มีอยู่ว่า เมื่อเข้าตาจน ทุกคนต่างก็เอาตัวรอดกันทั้งนั้นล่ะ ยิ่งจะต้องจ่ายเงินเยอะขนาดนั้น แก้ตัวไป เป็นใครก็ทำแบบนี้

ดังนั้น เมื่อองค์กรมีระเบียบเรื่องใดที่เกี่ยวกับการจัดการกับข้อมูลส่วนบุคคล ก็ดูให้ดีและปฏิบัติไปตามนั้น ในฐานะที่ท่านเองก็เป็นเจ้าของข้อมูลส่วนบุคคลด้วยเช่นกัน หากมีพนักงานขององค์กรใดที่ไม่ระมัดระวังการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน หรือมีองค์กรใดที่ท่านเป็นลูกค้า แล้วไม่มีมาตรการ ไม่สนใจดำเนินการตามกฎหมาย PDPA นี้ ท่านคิดว่าตัวเองจะยังคงเป็นลูกค้าอีกต่อไปหรือเปล่าล่ะ

ถ้าแต่ละคนที่มีหน้าที่ต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลของบุคคลอื่น ทำหน้าที่ของตนเองให้ดี ปฏิบัติตามกฎหมาย PDPA นี้อย่างเคร่งครัด เรื่องของการละเมิดข้อมูลส่วนบุคคลก็คงจะไม่เกิดขึ้น

ติดตามเรื่องนี้ได้ใน Youtube
ที่ QR Code นี้

5 ข้อมูลส่วนบุคคล (Personal Data) คืออะไร ?

ว่ากันตามความในมาตรา 6 ของกฎหมาย PDPA “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลหรือ Personal Data นี้ ขยายความได้ว่าเป็นข้อมูล สารสนเทศ เรื่องราวหรือข้อเท็จจริง อันทำให้สามารถระบุตัวตนของบุคคลธรรมดาคนหนึ่งใดได้ ไม่ว่าจะระบุทางตรงหรือระบุทางอ้อมก็ตาม และบุคคลนั้น ต้องไม่ใช่นิติบุคคล (บุคคลสมมติตามกฎหมาย) การกระทำต่อข้อมูลของนิติบุคคล ไม่ว่าจะอยู่ในรูปขององค์กรธุรกิจเช่น บริษัท ห้างร้านต่าง ๆ รวมทั้งองค์กรที่อาจจะไม่แสวงหากำไร อันได้แก่ มูลนิธิ สมาคมทั้งหลาย ตลอดไปจนถึงหน่วยงานของภาครัฐ (Public Authority) ก็ไม่เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมายนี้

อย่างไรก็ตาม มีเอกสารสำคัญของนิติบุคคลจำพวกที่ระบุตัวของกรรมการผู้มีอำนาจลงนามผูกพัน หรือกรรมการอื่น ซึ่งสามารถระบุตัวตนของบุคคลธรรมดาได้ ผู้เชียวชาญท่านระบุไว้ว่าข้อมูลเหล่านี้ ไม่ได้เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมาย PDPA แต่อย่างใด ในต่างประเทศที่ใช้กฎหมาย GDPR ก็มีแนวปฏิบัติที่ยึดถือเช่นนี้ กระนั้น ก็ไม่อาจสรุปได้ในทุกกรณีว่าข้อมูลของกรรมการผู้มีอำนาจนั้น จะไม่ใช่ข้อมูลส่วนบุคคลตามกฎหมาย PDPA เพราะหากเป็นข้อมูลของบุคคลที่ประกอบกิจการในรูปบุคคลธรรมดา แล้วไปทำนิติกรรมหรือสัญญาใดใดโดยไม่จดทะเบียนนิติบุคคลแล้ว ข้อมูลของผู้ประกอบการคนเดียวที่ว่านั้นก็เป็นข้อมลส่วนบุคคล

และที่สำคัญ บุคคลที่จะเป็นเจ้าของข้อมูลส่วนบุคคลได้นั้นจะต้องมี “สภาพเป็นบุคคลด้วย” หากตายไปแล้ว ก็ย่อมสิ้นสภาพของบุคคลไปตามที่กฎหมายกำหนดไว้ หรือกล่าวอย่างง่าย ๆ ก็คือบุคคล นอกเหนือจากจะไม่เป็นนิติบุคคลแล้ว จะต้องไม่ใช่คนตายที่หมดสภาพความเป็นบุคคลตามกฎหมายไปแล้วนั่นเอง

6 ข้อมูลส่วนบุคคลสองแบบ

ข้อมูลส่วนบุคคลมีสองแบบ ได้แก่ ข้อมูลส่วนบุคคลแบบทั่วไป (General Personal Data) เป็นข้อมูลทั่วไปที่เกี่ยวกับบุคคล เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ อีเมล ข้อมูลทางการเงิน ซึ่งว่ากันแบบ "ไม่กวน" ข้อมูลแบบนี้ ก็คือข้อมูลทั้งหลายที่ไม่ใช่ข้อมูลอ่อนไหวที่จะว่าในแบบที่ 2) และข้อมูลส่วนบุคคลแบบอ่อนไหว หรือเรียกสั้น ๆ ว่า ข้อมูลอ่อนไหว (Sensitive Personal Data) เป็นข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล ข้อมูลเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลต้องได้รับ "ความยินยอมโดยชัดแจ้ง" จากเจ้าของข้อมูล ทั้งนี้ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลแบบทั่วไป

6.1 ข้อมูลส่วนบุคคลแบบทั่วไป

พูดอย่างรวบรัดได้เช่นที่กล่าวข้างต้นว่า ข้อมูลส่วนบุคคลแบบทั่วไปนั้นก็คือ ข้อมูลส่วนบุคคลแบบที่ไม่ได้เป็นข้อมูลอ่อนไหวตามมาตรา 26 ของกฎหมาย PDPA นั่นเอง โดยเป็นข้อมูลส่วนบุคคลที่มีหลักทั่วไปในการจัดเก็บรวบรวมตามที่มาตรา 24 กำหนด เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์มือถือ เป็นต้น

6.2 ข้อมูลส่วนบุคคลแบบอ่อนไหว

ข้อมูลส่วนบุคคลแบบอ่อนไหวนี้ อันที่จริงไม่มีชื่อปรากฏอยู่ในกฎหมาย PDPA แต่อย่างใดเลย แต่เนื่องจากเราเองก็ได้รับอิทธิพลหรือเรียกว่านำเอากฎหมาย GDPR ของสหภาพยุโรปมาปรับใช้อย่างมาก เราก็นำเอาคำต่าง ๆ ที่มีใน GDPR เรื่องนี้มาใช้ด้วย ซึ่งในบทมาตราหลักของ GDPR ได้ใช้คำว่าข้อมูลส่วนบุคคลชนิดพิเศษ (Special Category of Personal Data) และในส่วนขยายคอยเจอคำว่า ข้อมูลส่วนบุคคลแบบอ่อนไหว (Sensitive

Personal Data) เราก็หยิบเอาคำหลังนี้มาใช้กันแพร่หลาย อันนี้ถือว่ารู้ไว้ใช่ว่ากับเรื่องที่มาของชื่อเรียกของคำที่เราท่านคุ้นหาก็แล้วกันนะ

ตามกฎหมาย PDPA นั้นมีอยู่ 12 อย่างได้แก่

1) เชื้อชาติ
2) เผ่าพันธุ์
3) ความคิดเห็นทางการเมือง
4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
5) พฤติกรรมทางเพศ
6) ประวัติอาชญากรรม
7) ข้อมูลสุขภาพ
8) ข้อมูลความพิการ
9) ข้อมูลสหภาพแรงงาน (การเป็นสมาชิกสหภาพแรงงาน เป็นต้น)
10) ข้อมูลพันธุกรรม
11) ข้อมูลชีวภาพ (Biometric Data เช่น ข้อมูลสแกนม่านตา ข้อมูลสแกนลายนิ้วมือ เป็นต้น)
12) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลที่จะประกาศต่อไป ซึ่งในอนาคตทางคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็อาจจะกำหนดให้ข้อมูลส่วนบุคคลบางรายการเช่น ประวัติการลงโทษทางวินัยของพนักงาน ข้อมูลค่าจ้าง เงินเดือน ค่าตอบแทนของพนักงาน เป็นข้อมูลอ่อนไหวเพิ่มเติมก็เป็นได้ อันนี้ก็ต้องรอฟังจากประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต่อไป

ข้อมูลส่วนบุคคล (Personal Data) นี่มีเยอะมาก มีทั้งข้อมูลส่วนบุคคลของพนักงาน ข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลส่วนบุคคลของคู่ค้า ซึ่งนับเป็นเรื่องที่เราจะต้องไปค้นหาให้ได้ว่ามีข้อมูลส่วนบุคคลของใคร เก็บไว้ที่ใดบ้างในฐานข้อมูล .oไฟล์ หรือระบบอะไรต่าง ๆ จากนั้นก็ต้องมากำหนดฐานการประมวลผลข้อมูลส่วนบุคคล (Data Processing Lawful Basis) และไปดำเนินการอื่นตามที่กฎหมาย

กำหนดไว้ต่อไป

เพื่อให้เห็นภาพ อยากยกตัวอย่างข้อมูลส่วนบุคคลของลูกค้าหรือคู่ค้า ลองมาดูกัน

(1) ข้อมูลสำเนาเอกสารที่สามารถใช้เพื่อระบุตัวตนของลูกค้าหรือคู่ค้า ซึ่งเราต้องนำมาประกอบการให้บริการ หรือการทำงานร่วมกัน เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง เอกสารอื่น ๆ ที่ออกให้โดยหน่วยงานของรัฐ ทะเบียนราษฎร

(2) ข้อมูลในการติดต่อของลูกค้าหรือคู่ค้า เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล์ ข้อมูลโซเชียลมีเดีย (เฉพาะที่เป็นบุคคลธรรมดา)

(3) ข้อมูลเกี่ยวกับตัวของลูกค้าหรือคู่ค้า เช่น วันเดือนปีเกิด อายุ เพศ สถานะการสมรส ความสนใจ ความคิดเห็นทางการเมือง

(4) ข้อมูลเกี่ยวกับสมาชิกครอบครัวหรือผู้อยู่ในความดูแลของลูกค้าหรือคู่ค้าที่มีสิทธิได้รับประโยชน์จากสินค้าหรือบริการ เช่น ข้อมูลเกี่ยวกับคู่สมรส ข้อมูลเกี่ยวกข้อมูลเกี่ยวกับบิดามารดา ผู้รับผลประโยชน์ เป็นต้น

(5) ข้อมูลเกี่ยวกับการศึกษา ความสามารถ และท่านสมบัติอื่น ๆ ของลูกค้าหรือคู่ค้า เช่น ระดับการศึกษา วุฒิการศึกษา สถาบัน/มหาวิทยาลัย ประวัติการศึกษา ประวัติการฝึกผลการศึกษา ผลการทดสอบความสามารถอื่น ๆ ทีเราต้องใช้เพื่อการให้บริการหรือทำงานด้วย

(6) ข้อมูลเกี่ยวกับประสบการณ์ทำงาน หรือประสบการณ์การให้บริการของลูกค้าหรือคู่ค้าแล้วแต่จะจัดเก็บ

บางทีเราก็จะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือคู่ค้าอีกส่วนหนึ่งที่เป็นข้อมูลอ่อนไหวหรือ Sensitive Data ได้แก่ ข้อมูลสุขภาพ เช่น น้ำหนัก ส่วนสูง โรคประจำตัว โรคตาบอดสี ผลการตรวจร่างกาย ข้อมูลการแพ้อาหาร ข้อมูลการแพ้ยา หมู่โลหิต ใบรับรองแพทย์ ประวัติการรักษาพยาบาล ประวัติการ

รักษาพยาบาล และข้อมูลชีวภาพ (Biometric Data) เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ ข้อมูลจำลองม่านตา ข้อมูลอัตลักษณ์เสียง เพื่อวัตถุประสงค์ในการพิสูจน์และยืนยันตัวตนของลูกค้าบริการที่ขอสมัคร และ/หรือ ทำธุรกรรมผ่านช่องทางต่าง ๆ ทีองค์กรให้บริการ หรือของคู่ค้าที่จะต้องใช้ประสานงานกับองค์กร เป็นต้น

คราวนี้มาลองดูข้อมูลส่วนบุคคลของพนักงานหรือบุคลากรของเรา ก็มีหลากหลายอย่างมากไม่แพ้กัน ที่ว่ามันมีหลากหลายนั้นก็เพราะข้อมูลส่วนบุคคลหมายถึงข้อมูลสารสนเทศใด ที่นำมาใช้ระบุตัวตนของบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม ก็เข้าข่ายเป็นข้อมูลส่วนบุคคลทั้งนั้น เราได้ลองรวบรวมมาโดยแยกไว้ตามรูปแบบของข้อมูลเพื่อยืนยันว่า มันเยอะจริง ๆ

1) ข้อมูลรายละเอียดส่วนตัว เช่น คำนำหน้าชื่อ ชื่อ-นามสกุล เพศ วันเกิด อายุ หมู่เลือด สัญชาติ ภูมิลำเนาที่เกิด ลายมือชื่อ สถานภาพการสมรส จำนวนบุตร ประวัติทางราชการทหาร ประวัติการอุปสมบท ข้อมูลเกี่ยวกับเอกสารที่รัฐบาลออกให้ (เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง วีซ่า หมายเลขประจำตัวผู้เสียภาษี ใบอนุญาตทำงาน สำเนาทะเบียนบ้าน รูปถ่ายเอกสารแสดงการเปลี่ยนชื่อ/นามสกุล) เลขสะสมไมล์สายการบิน หมายเลขทะเบียนรถยนต์ สี และรุ่นของรถยนต์ รายละเอียดบัญชีธนาคาร เลขที่บัตรเครดิต และเลขสำหรับรักษาความปลอดภัยหลังบัตรเครดิต ประวัติการดำรงตำแหน่งทางการเมือง ข้อมูลหลักทรัพย์ค้ำประกัน ประวัติเครดิตบูโร หลักฐานการชำระภาษี การตรวจสอบประวัติทางการเงิน เป็นต้น

2) ข้อมูลการติดต่อ เช่น ที่อยู่ไปรษณีย์ตามบัตรประจำตัวประชาชน หรือทะเบียนบ้าน ที่อยู่ไปรษณีย์ปัจจุบัน ที่อยู่ไปรษณีย์ของที่ทำงาน หมายเลขโทรศัพท์ หมายเลขโทรสาร ที่อยู่อีเมล บัญชีผู้ใช้งานสื่อสังคมออนไลน์ ช่องทางการติดต่อผ่านสื่อสังคมออนไลน์ และข้อมูลจากเครือข่ายสังคมออนไลน์ ข้อมูลที่อยู่ของนักเรียนทุนที่เดินทางไปศึกษาต่อต่างประเทศ

3) ข้อมูลการศึกษา เช่น ท่านวุฒิการศึกษา ข้อมูลหลักฐานแสดงท่านวุฒิทางการศึกษา สถานศึกษา/สถาบัน สาขาวิชาวิชาเอก ปีที่สำเร็จการศึกษา คะแนนเฉลี่ยสะสม สำเนาใบแสดงผล

การศึกษา สำเนาใบปริญญาบัตร หลักสูตรการฝึกอบรม/สัมมนาที่เกี่ยวข้อง ประกาศนียบัตร/ท่านวุฒิพิเศษ สถาบันที่มีการอบรม ระยะเวลาอบรม ปีที่อบรม ข้อมูลเพื่ อใช้บริหารจัดการด้านทุนการศึกษา ได้แก่ ผลการทดสอบที่ใช้สำหรับศึกษาต่อในประเทศและต่างประเทศ ข้อมูลตอบรับจากทางสถาบันการศึกษาในต่างประเทศ เป็นต้น

4) ข้อมูลการจ้างงานและการทำงาน เช่น รหัสพนักงาน User ID/รหัสผ่านตั้งต้น ข้อมูลบัตรประจำตัวพนักงาน ตำแหน่งสายงาน ชื่อหน่วยงาน รหัสสังกัด ระยะเวลาในการทำงาน ข้อมูลบันทึกเวลาทำงาน เงินเดือน เอกสารแสดงรายได้ หนังสือรับรองการทำงานจากสถานที่ทำงานเดิม รายการการลงทุน/สัญญา ข้อมูลบริษัท/ธุรกิจที่เกี่ยวข้อง รายงานการมีส่วนได้เสียในนิติบุคคลอื่น ข้อมูลการถือหุ้นในนิติบุคคลต่าง ๆ รายงานการถือหลักทรัพย์ของธนาคาร หลักฐานแสดงการชำระภาษีเงินได้ ข้อมูลเกี่ยวกับใบอนุญาตทำงาน (เช่น เลขที่บัตรใบอนุญาต วันที่ออกบัตรและวันหมดอายุบัตร ประวัติการสอบและผลการสอบ) ประสบการณ์ทำงาน (เช่น สถานที่ทำงาน (ปัจจุบัน/อดีต) อาชีพ ตำแหน่ง วันที่เริ่มทำงาน วันที่สิ้นสุดการทำงาน อายุงาน) สถานภาพการจ้างงาน ผลการตรวจหาสารเสพติด ข้อมูลการตรวจสอบบุคคลอ้างอิง ข้อมูลหมายเลขประจำตัวผู้เสียภาษี ข้อเรียกร้องประกันภัยเงินทดแทนแรงงาน ประวัติการจ้างงาน วันที่เริ่มว่าจ้าง การเลิกจ้าง ทรัพย์สินที่อยู่ในความครอบครองระหว่างการจ้างงาน ข้อมูลการประเมินต่าง ๆ เช่นการประเมินผลการปฏิบัติงาน การประเมินสมรรถนะเพื่อการวางแผนพัฒนาบุคลากรเป็นรายบุคคล เป็นต้น

5) ข้อมูลเกี่ยวกับเงินเดือนและสวัสดิการ เช่น บันทึกเงินเดือน (เช่น เงินเดือน/รายได้ต่อเดือน รายละเอียดค่าตอบแทน ระดับเงินเดือน โบนัส) ค่าใช้จ่าย ค่าตอบแทน ค่านายหน้า ค่าทำงานล่วงเวลา ค่าทำงานกะ ค่ารักษาพยาบาล ค่าทำงานนอกสถานที่ ค่าเดินทาง เงินค่าตอบแทนพิเศษ และสวัสดิการ ข้อมูลการหักเงิน (เช่น สำหรับกองทุนสำรองเลี้ยงชีพ ภาษี ประกันสังคม) เงินชดเชย และเงินบำนาญ เป็นต้น

6) ข้อมูลเกี่ยวกับการเงิน เช่น ข้อมูลสถานะและประวัติทางการเงิน ข้อมูลเกี่ยวกับการตรวจสอบประวัติ หมายเลขบัญชีที่มีกับสถาบันการเงิน ประวัติการทำธุรกรรมทางการเงิน ประวัติ

สินเชื่อ ข้อมูลการลงทุน เป็นต้น

หากจะเจาะจงลงไปที่ข้อมูลส่วนบุคคลของพนักงานที่เป็นข้อมูลอ่อนไหว หรือ Sensitive Data ก็ได้แก่

1) ข้อมูลสุขภาพ เช่น น้ำหนัก ส่วนสูง โรคประจำตัว โรคตาบอดสี ผลการตรวจร่างกาย ข้อมูลการแพ้อาหาร ข้อมูลการแพ้ยา หมู่โลหิต ใบรับรองแพทย์ ประวัติการรักษาพยาบาล ประวัติการรักษาพยาบาล
2) ข้อมูลชีวภาพ (Biometric Data) เช่น ข้อมูลจำลองลายนิ้วมือ ข้อมูลภาพจำลองใบหน้า เพื่อใช้ในการระบุและยืนยันตัวตนของพนักงาน ป้องกันอาชญากรรม เป็นต้น
3) ข้อมูลเกี่ยวกับประวัติอาชญากรรม (Criminal Record)
4) ข้อมูลเกี่ยวกับความเชื่อในลัทธิศาสนา ปรัชญา
5) ข้อมูลเชื้อชาติ สัญชาติ
6) ข้อมูลความพิการของบุคคล อันมักจะปรากฏเป็นหนังสือรับรองผู้พิการ และบัตรประจำตัวผู้พิการ เป็นต้น
7) ข้อมูลการเป็นสมาชิกสหภาพแรงงาน รวมถึงการดำเนินกิจกรรมของสหภาพแรงงาน
8) ข้อมูลพันธุกรรม (Genetic Data)

ที่ว่ามานี้คงเป็นเพียงส่วนหนึ่งเท่านั้น ข้อมูลส่วนบุคคลของลูกค้าและคู่ค้า จะมีเยอะมาก ซึ่งไม่ว่าจะมาก หรือไม่มากเพียงใดก็ตาม ก็ต้องหาให้พบทั้งหมด ซึ่งหลายองค์กรก็จะใช้ Software การค้นหาและวิเคราะห์ข้อมูลเช่น Data Discovery Software มาช่วยซึ่งก็ควรต้องเป็นแบบนั้นล่ะ

7 บุคคล 3 ฝ่ายที่เกี่ยวข้องกับกฎหมาย PDPA

ตัวละครสำคัญ 3 ฝ่ายในกฎหมาย PDPA นั้นเห็นจะได้แก่ตามภาพนี่ล่ะ ซึ่งต้องมาศึกษาเสียหน่อยว่า แต่ละฝ่าย มีบทบาทหน้าที่อย่างไรบ้าง

เจ้าของข้อมูลส่วนบุคคล
(Data Subject)

ผู้ควบคุมข้อมูลส่วนบุคคล
(Data Controller)

ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data Processor)

7.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เริ่มต้นที่ตัวเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนเลย เจ้าของข้อมูลส่วนบุคคล หรือต่อไปจะเรียกย่อ ๆ ว่า "DS" นั้น หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของข้อมูล (Ownership) หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลนี้จะหมายถึงบุคคลธรรมดาเท่านั้น ไม่รวมถึง "นิติบุคคล" (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท สมาคม มูลนิธิ หรือองค์กรอื่นใด

เจ้าของข้อมูลส่วนบุคคล ได้แก่บุคคลดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะ หมายถึง

1.1) บุคคลที่มีอายุตั้งแต่ 20 ปีบริบูรณ์ขึ้นไป หรือ

1.2) ผู้ที่สมรสตั้งแต่อายุ 17 ปีบริบูรณ์ขึ้นไป หรือ

1.3) ผู้ที่สมรสก่อนอายุ 17 ปี โดยศาลอนุญาตให้ทำการสมรส หรือ

1.4) ผู้เยาว์ซึ่งผู้แทนโดยชอบธรรมให้ความยินยอมในการประกอบธุรกิจทางการค้าหรือธุรกิจอื่น หรือในการทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน ในความเกี่ยวพันกับการประกอบธุรกิจหรือ การจ้างแรงงานข้างต้นให้ผู้เยาว์มีฐานะเสมือนดังบุคคล