

PDPA *step-by-step* สำหรับงาน HR

กฎหมายคุ้มครองข้อมูลส่วนบุคคล



8 ขั้นตอนกับการ Implement PDPA
แบบเข้าใจง่าย และเอาไปทำได้ไม่ยาก
สำหรับงาน HR โดยเฉพาะ

ดร.ชัชวาล อรวงศ์ศุภกัต
นักจัดการคุ้มครองข้อมูลส่วนบุคคลระดับ 6, TPQI
วิทยากรและที่ปรึกษา PDPA

PDPA

step-by-step

สำหรับงาน **HR**

ชัชวาล อรวงศ์ศุภทัต
นักจัดการคุ้มครองข้อมูลส่วนบุคคล ระดับ 6
วิทยากรและที่ปรึกษา PDPA

PDPA step-by-step

สำหรับงาน HR

ข้อมูลทางบรรณานุกรม

ชัชวาล อรวงศ์ศุภกัต

PDPA step-by-step สำหรับงาน HR—

กรุงเทพฯ: ไอดี ออล ดิจิตอลพริ้นท์, 2566

ISBN : 978-616-604-966-4

สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537

ห้ามลอกเลียนแบบไม่ว่าส่วนหนึ่งส่วนใดของหนังสือเล่มนี้
ไม่ว่ารูปแบบใดๆ นอกจากจะได้รับอนุญาต เป็นลายลักษณ์อักษร
จากผู้เขียนเท่านั้น

บรรณาธิการ : ชัชวาล อรวงศ์ศุภกัต

จัดทำรูปเล่ม : ชัชวาล อรวงศ์ศุภกัต

ออกแบบปกโดย : ธรรมภัทร์ โสภณดิษย์

รูปเล่ม : ธรรมภัทร์ โสภณดิษย์

พิสูจน์อักษร : สุราสินี ตั้งแสง

จัดทำโดย : ชัชวาล อรวงศ์ศุภกัต

142/129 หมู่ที่ 5 ถนนสวนผัก 32 ตำบลมหาสวัสดิ์

อำเภอบางกรวย จังหวัดนนทบุรี 11130

พิมพ์ที่ : บริษัท ไอดี ออล ดิจิตอลพริ้นท์ จำกัด

52 ซอยเอกชัย 69 ถนนเอกชัย แขวง-เขตบางบอน กทม. 10150

โทรศัพท์ : 02-8995429-35

Email : office2@ideol-print.com

จำนวนหน้า : 384 หน้า

ความนำ

PDPA step-by-step สำหรับงาน HR

ในบรรดาหน่วยงานที่ต้องทำ PDPA Compliance ฝ่ายหรือแผนก HR นับได้ว่าเป็นหน่วยงานภายในองค์กรที่ต้องทำอะไรทั้งหลายให้สอดคล้องกับกฎหมายมากที่สุด และด้วยความที่เป็นหน่วยงานสนับสนุนภายในองค์กร HR ของหลายองค์กรก็จะทำหน้าที่อีกอย่างหนึ่งที่สำคัญคือการเป็นพี่เลี้ยงขององค์กรอื่น support บุคลากรหลักคือ DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการทำ PDPA ของหน่วยงานอื่นภายใน นี่คือเหตุผลประการหลักที่ HR จำเป็นอย่างมากที่จะต้องอ่านหนังสือเล่มนี้ของเรา หลายท่านบอกว่า PDPA ในองค์กรทำไม่ยากหรอก !! อันที่จริงก็ไม่ได้ยากมากนัก หากมองในแง่การทำเอกสารบางตัว เช่นการทำ Privacy Notice ประกาศให้เจ้าของข้อมูลส่วนบุคคลทราบตามที่กฎหมายกำหนด แต่หากจะทำให้สอดคล้องกับกฎหมายทั้งระบบแล้วละ เรื่องนี้ไม่ง่ายเลยทีเดียว และยังมีมิติของ “ความเยาะ” ในสิ่งที่ต้องทำอีกด้วย อย่างไรก็ตาม เราก็เชื่อว่า หนังสือเล่มนี้ จะเป็นแนวทางให้ท่านทั้งหลายที่ทำงาน HR ใช้เป็นแนวทางในการทำ PDPA Compliance หรือ ทำ PDPA Implementation ในองค์กรอย่างได้ผล ประหยัดงบประมาณขององค์กรด้วยการลงมือทำเอง ขอเพียงแต่ท่านตั้งใจ มุ่งมั่นลงมือทำ ซึ่งตลอดระยะหรือในแต่ละขั้นตอนของการทำ Implementation ที่ปรากฏในหนังสือเล่มนี้ ย่อมไม่ยากที่จะลงมือทำ แต่ก็ไม่ยากหากท่านใช้ “ความพยายาม” ในการลงมือทำอย่างต่อเนื่อง แนวทางของเราก็เป็นอีกแนวทางหนึ่งที่เราได้ทดลองทำมาในหลายองค์กรแล้วพบว่าได้รับการยอมรับจากแผนกต่าง ๆ ที่เกี่ยวข้องว่าไม่ยากที่จะเข้าใจ และครบถ้วนตามที่กฎหมายกำหนดไว้

ดร.ชัชวาล อรวงศ์ศุภกัตต
ธันวาคม 2566

สารบัญ

PDPA step-by-step สำหรับงาน HR

เรื่องที่ต้องรู้ก่อน Implement PDPA ในงาน HR

(1) ข้อมูลส่วนบุคคล (Personal Data)	1
(2) รูปแบบและประเภทของข้อมูลส่วนบุคคล	10
(3) เจ้าของข้อมูลส่วนบุคคล	26
(4) ผู้ควบคุมข้อมูลส่วนบุคคล	31
(5) ผู้ประมวลผลข้อมูลส่วนบุคคล	38
(6) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	44
(7) ฐานทางกฎหมายสำหรับการประมวลผล ข้อมูลส่วนบุคคล	48
(8) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล และ ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล	91
(9) มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ส่วนบุคคล	109
(10) การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล	121
(11) การบันทึกการกิจกรรมการประมวลผล ข้อมูลส่วนบุคคล	133
(12) การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ	147
(13) ความรับผิดชอบตามกฎหมาย PDPA	156

สารบัญ

(ต่อ)

8 ขั้นตอนของการทำ PDPA ในงาน HR แบบ step-by-step	166
(1) ระบุงิจกรรมงาน	185
(2) ระบุนายการข้อมูลส่วนบุคคลตามกิจกรรมงาน	194
(3) กำหนดประเภทของข้อมูลส่วนบุคคล	202
(4) จัดทำบันทึกรายการ (Record of Processing Activity - RoPA)	210
(5) จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) ในงาน HR	230
(6) จัดทำและนำเอาแบบฟอร์มขอความยินยอม (Consent Form) มาปรับใช้	242
(7) จัดทำมาตรการและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด	251
(8) ปรับปรุงขั้นตอนหรือกระบวนการทำงาน HR	280
ภาคผนวก	
ตัวอย่างประกาศความเป็นส่วนตัวที่ HR เกี่ยวข้อง	324
รู้จักผู้เขียน	378

หนังสือแนะนำ PDPA for Recruitment

PDPA for Recruitment

เจาะลึกแนวทางการ Implement PDPA
ในงาน Recruitment & Selection แบบเล่มเดียวจบ
พร้อมตัวอย่างเอกสารที่นำไปปรับใช้ได้จริง



กฎหมายคุ้มครองข้อมูลส่วนบุคคล

หลักกฎหมาย ถาม-ตอบหลากหลายเรื่องคาใจ และแนวทางการ
Implement PDPA ในงาน Recruitment & Selection

ดร.ชัชวาล อรวงศ์ศุภกิต
ประพนธ์ กิจอำไพวงศ์
วิทยากรและที่ปรึกษา PDPA

ดร.ชัชวาล อรวงศ์ศุภกิต

หนังสือ “ขายดี” เล่มใหม่ 100 เรื่องตามตอบ PDPA ในงาน HR

100 เรื่องตามตอบ PDPA ในงาน HR

กฎหมายคุ้มครองข้อมูลส่วนบุคคล
ในงานบริหารทรัพยากรบุคคล



100 คำถามตอบเกี่ยวกับ PDPA ในงานบริหารทรัพยากรบุคคล
ที่คำถามมาเราตอบในช่องทางต่าง ๆ ที่รวบรวมมาอย่างครบถ้วน

ตอบจากประสบการณ์ที่ปรึกษา PDPA อย่างละเอียด

ดร.ชัชวาล อรวงศ์ศุภกิตต์
ประพนธ์ กิจอำไพวงศ์

ดร.ชัชวาล อรวงศ์ศุภกิตต์

(1)
ข้อมูลส่วนบุคคล
(Personal Data)

PDPA

Personal Data Protection Act

พระราชบัญญัติ
คุ้มครอง
ข้อมูลส่วนบุคคล

กฎหมาย PDPA หรือที่เราเรียกกันสั้น ๆ ว่า PDPA นั้น ก็คือกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือในภาษาอังกฤษก็จะเรียกว่า Personal Data Protection Act นั้น ตราขึ้นมาตั้งแต่ปี พ.ศ.2562 ที่ผ่านมา กฎหมายนี้ มีขึ้นเพื่อกำหนดหลักเกณฑ์ กลไกและมาตรการในการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ในอันที่จะห้ามเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือไม่มีอำนาจที่กฎหมายบัญญัติเอาไว้ให้สามารถดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้โดยไม่ต้องขอความยินยอม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมาย PDPA นี้ อันที่จริงไม่ได้บังคับใช้กับทุกองค์กร และผู้ควบคุมข้อมูลส่วนบุคคลจำนวนหนึ่งที่ไม่ต้องบังคับตามกฎหมาย ซึ่งกำหนดไว้เรียบร้อยแล้วในมาตรา 4 อันได้แก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อมูลส่วนบุคคล

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการ สื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการ แล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

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

และหากพิจารณากันว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมาย PDPA นี้สำคัญกับองค์กรอย่างไร

เห็นที่ต้องคุยกันในมุมของประโยชน์ที่องค์กรจะได้รับจากการปฏิบัติหรือดำเนินการตามกฎหมายที่ว่านี้ ซึ่งผู้รู้ท่านก็แนะนำไว้ในทำนองที่สอดคล้องกันเช่น

(1) การมีกฎหมายนี้ย่อมช่วยเพิ่มความเชื่อมั่นในมาตรฐานของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อคู่ค้า ลูกค้าหรือพันธมิตรในการดำเนินงานขององค์กรไม่ว่าจะในระดับประเทศหรือระดับนานาชาติ หากเป็นองค์กรภาคธุรกิจเอกชนที่ดำเนินธุรกิจ在不同ประเทศที่เค้านับถือใช้กฎหมายลักษณะนี้ด้วยแล้ว ก็ย่อมที่จะเป็นตัวช่วยสร้างความเชื่อมั่นในการค้าขายระหว่างกันในทางหนึ่ง และที่ว่าไปนี้ หากจะกล่าวว่าเป็นการเพิ่มขีดความสามารถในการแข่งขันขององค์กรก็ไม่ผิดนัก

ประเด็นมีอยู่ว่า แล้วไม่ทำตามกฎหมาย PDPA จะเกิดอะไรขึ้น ?

ตอบกันง่าย ๆ ตรงนี้เลยว่าก็ผิดกฎหมาย PDPA นั่นเอง และตัวกฎหมายนี้ก็มิโทษสามแบบเลย ทั้งโทษอาญา (ปรับและจำคุก) โทษปรับทางปกครอง และโทษหรือความรับผิดชอบทางแพ่งจากการทำให้บุคคลอื่นได้รับความเสียหายทางละเมิด ที่สำคัญนั้นอยากให้ดูมาตรา 81 ซึ่งสรุปความจากตัวบทกฎหมายได้ว่า หากผู้กระทำผิดกฎหมายนี้เป็นนิติบุคคล (ก็คือบริษัท หรือองค์กรภาครัฐที่ต้องปฏิบัติตามกฎหมายทั้งหลายนั้นละ) อันเป็นการกระทำผิดที่เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลนั้นมีหน้าที่ต้องสั่งการ หรือกระทำการ หรือละเว้นไม่สั่ง

ข้อมูลส่วนบุคคล

การหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด ผู้นำ ซึ่งก็หมายถึงกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ต้องรับโทษตามที่บัญญัติสำหรับความผิดนั้น ๆ ด้วย โดยเฉพาะหากความผิดตามกฎหมาย PDPA นั้นมีโทษจำคุก บุคคลที่เป็นกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล ก็อาจจะต้องรับโทษจำคุกด้วย

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

เพราะจำคุกนิติบุคคลไม่ได้ ก็ต้องจำคุกเอาที่กรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนี้ละ

ถ้าแบบนี้ ก็ระมัดระวังกันเสียหน่อย จะเอาหูไปนา เอาตาไปไร่ ไม่ใส่ใจสนใจกฎหมาย PDPA แล้วหากเกิดปัญหาการละเมิดข้อมูลส่วนบุคคลของใครก็ตาม ไม่ว่าจะป็นลูกค้า พนักงาน ผู้สมัครงาน ก็อาจจะเคลียร์ไม่ไหว ตั้งรับไม่ทันสถานการณ์ก็ได้ เราแนะนำว่าอย่าประมาทไป เดี่ยวจะเข้าทำนองเสียหน่อยเสียยาก เสียมาก เสียง่าย และบานปลายไปถึงเรื่องการเสื่อมเสีย

ข้อมูลส่วนบุคคล

ภาพลักษณ์ขององค์กร ซึ่งก็ต้องยอมรับกันว่า กว่าจะสร้างภาพลักษณ์องค์กรให้ดีงามได้มาจนถึงวันนี้ มันไม่ง่ายและใช้งบประมาณไปก็น่าจะไม่น้อย แต่อาจจะต้องมาเสียไปแบบง่าย ๆ เพียงเพราะอารมณ์ประมาณว่าเสียเวลา

ยิ่งกับผู้บริหารมืออาชีพที่องค์กรเค้าว่าจ้างมาทำงาน ย่อมเป็นที่คาดหวังว่าจะต้องไม่ทำผิดกฎหมายเสียเอง แต่ด้วยความบางท่านก็คิดแต่ว่าเสียเวลาทำมาหารายได้ ทำตามกฎหมาย PDPA มีแต่เสียเงิน หากเกิดเรื่องราวละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมา ก็อาจจะถูกเล่นงานหนักจากผู้ถือหุ้นที่เป็นเจ้าขององค์กรตัวจริงเอาได้ นำเสียตายความเป็นนักบริหารมืออาชีพแต่ต้องมาตกม้าตายกับเรื่องที่ไม่ทำตามกฎหมาย PDPA นี้

ผู้ประกอบการหลายท่านไม่ได้สนใจกฎหมาย PDPA เพราะเคยมีประสบการณ์กับกฎหมายความปลอดภัยมาแล้วพบว่าไม่มีใครมาตรวจสอบว่าองค์กรได้ทำเรื่องความปลอดภัย อาชีวอนามัยและสภาพแวดล้อมในการทำงานหรือไม่ เพียงใดก็เลยชะล่าใจ เพราะลำพังพนักงานไม่มีใครไปร้องเรียนอยู่แล้ว แต่กับกฎหมาย PDPA เจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มีแต่พนักงานอย่างเดียว ยังมีลูกค้า คู่ค้า และผู้สมครงานอีกด้วย เราจะทำงานแบบ “วัดใจ” กับบุคคลเหล่านี้หรือไม่ว่าเขาจะไม่ไปร้องเรียนการกระทำผิดกฎหมาย PDPA ขององค์กรของเรา

เมื่อมีปัญหาเช่น ข้อมูลส่วนบุคคลอ่อนไหวของลูกค้ารั่วไหลไป และมีเรื่องร้องเรียนขึ้นมา ฟ้องร้องกัน

ข้อมูลส่วนบุคคล

ตามติดต่อเนื่อง ก็อย่าไวยวายไปเอาเรื่องไปราวกับพนักงานละ เพราะตอนที่พนักงานบอกให้ผู้ประกอบการทำ ผู้ประกอบการบอกว่าเปลืองเงินเปลืองทองไม่ยากทำ

สำหรับพนักงาน ที่จะต้องระมัดระวังการปฏิบัติตามกฎหมายนั้น ก็อยากจะบอกว่า แม้พนักงานมีฐานะเป็นผู้ทำการแทนผู้ควบคุมข้อมูลส่วนบุคคล ก็ไม่ใช่ว่านี่ก็อยากจะทำอะไรก็ตาม หรือไม่สนใจใยดีที่จะปฏิบัติตามกฎหมาย หรือปล่อยปละละเลยไม่ดูแลรักษาข้อมูลส่วนบุคคลที่ตนเกี่ยวข้อง จนเกิดปัญหาข้อมูลรั่วไหลแล้วเกิดความเสียหายกับเจ้าของข้อมูลส่วนบุคคล หากเกิดสถานการณ์เช่นนั้นขึ้น ท่านคิดว่าเจ้าของข้อมูลส่วนบุคคลที่เขาเดือดร้อน นอกจากเขาจะร้องเรียนหรือฟ้องร้ององค์กรแล้ว เขาจะฟ้องฟ้องร้องผู้ปฏิบัติงานเข้าไปด้วยหรือไม่

พันรชัวร์ ๆ ได้ว่าฟ้องฟ้องเข้าไปแน่นอน และถึงจุดนั้น เดิมที่เป็นอยู่ว่า องค์กรหรือผู้บริหารระดับสูง ไม่ค่อยสนใจที่จะปฏิบัติตามกฎหมาย PDPA เมื่อจะถูกปรับสัก 3 ล้านบาท เพราะทำผิดกฎหมาย PDPA ท่านคิดว่าบริษัททั้งหลาย เขาจะส่งทนายความไปให้การว่าเขาสนใจหรือไม่สนใจที่จะปฏิบัติตามกฎหมายละ เรื่องแบบนี้ ท่านคิดว่าไม่ยากโดยไม่ต้องพึ่งพ่อบุญหรือแม่บุญพ่อบุญคนใดมาพันรชัวร์แต่อย่างใดเลย

แล้วก็เป็นไปได้มากเลยที่ห่วยจะออกที่ท่าน เพราะองค์กรก็อาจจะบอกว่า ท่านไม่ปฏิบัติตามระเบียบหรือกฎกติกาตามที่องค์กรออกไว้ตามกฎหมาย กลายเป็นงานเข้าตัวท่านเอง แม้องค์กรในฐานะนายจ้างจะช่วย

ข้อมูลส่วนบุคคล

จ่ายค่าสินไหมทดแทนนั้นให้กับผู้เสียหาย ท่านคิดว่า
องค์กรจะ ไล่เบี้ยเอาากับท่าน หรือเปล่าละ ทั้ง ๆ ที่อันที่
จริง องค์กรเองนั้นละไม่สนใจที่จะทำตามกฎหมาย

*อุทาหรณ์เรื่องนี้มือยู่ว่า เมื่อเข้าตาจน ทุกคนต่าง
ก็เอาตัวรอดกันทั้งนั้นละ ยังจะต้องจ่ายเงินเยอะขนาด
นั้น แก่ตัวไป เป็นใครก็ทำแบบนี้*

ดังนั้น เมื่อองค์กรมีระเบียบเรื่องใดที่เกี่ยวกับการ
จัดการกับข้อมูลส่วนบุคคล ก็ดูให้ดีและปฏิบัติไปตามนั้น
ในฐานะที่ท่านเองก็เป็นเจ้าของข้อมูลส่วนบุคคลด้วย
เช่นกัน หากมีพนักงานขององค์กรใดที่ไม่ระมัดระวังการ
เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน
หรือมีองค์กรใดที่ท่านเป็นลูกค้า แล้วไม่มีมาตรการ ไม่
สนใจดำเนินการตามกฎหมาย PDPA นี้ ท่านคิดว่า
ตัวเองจะยังคงเป็นลูกค้าอีกต่อไปหรือเปล่าละ

ถ้าแต่ละคนที่มีหน้าที่ต้องเกี่ยวข้องกับข้อมูลส่วน
บุคคลของบุคคลอื่น ทำหน้าที่ของตนเองให้ดี ปฏิบัติ
ตามกฎหมาย PDPA นี้อย่างเคร่งครัด เรื่องของการ
ละเมิดข้อมูลส่วนบุคคลก็คงจะไม่เกิดขึ้น

*แล้วข้อมูลส่วนบุคคล (Personal Data) คือ
อะไร ?*

ตอบเรื่องนี้ตามความในมาตรา 6 ของกฎหมาย
PDPA “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูล
เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่า
ทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่
กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลหรือ Personal Data นี้ ขยายความได้ว่าเป็นข้อมูล สารสนเทศ เรื่องราวหรือข้อเท็จจริง อันทำให้สามารถระบุตัวตนของบุคคลธรรมดาคนหนึ่งได้ได้ ไม่ว่าจะเป็นระบุทางตรงหรือระบุทางอ้อมก็ตาม และบุคคลนั้น ต้องไม่ใช่นิติบุคคล (บุคคลสมมติตามกฎหมาย) การกระทำต่อข้อมูลของนิติบุคคล ไม่ว่าจะอยู่ในรูปขององค์กรธุรกิจเช่น บริษัท ห้างร้านต่าง ๆ รวมทั้งองค์กรที่อาจจะไม่แสวงหากำไร อันได้แก่ มูลนิธิ สมาคมทั้งหลาย ตลอดไปจนถึงหน่วยงานของภาครัฐ (Public Authority) ก็ไม่เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมายนี้ อย่างไรก็ตาม มีเอกสารสำคัญของนิติบุคคลจำพวกที่ระบุตัวของกรรมการผู้มีอำนาจลงนามผูกพัน หรือกรรมการอื่น ซึ่งสามารถระบุตัวตนของบุคคลธรรมดาได้ ผู้เชี่ยวชาญท่านระบุไว้ว่า ข้อมูลเหล่านี้ ไม่ได้เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมาย PDPA แต่อย่างใด ในต่างประเทศที่ใช้กฎหมาย GDPR ก็มีแนวปฏิบัติที่ยึดถือเช่นนี้ กระนั้น ก็ไม่อาจสรุปได้ในทุกกรณีว่าข้อมูลของกรรมการผู้มีอำนาจนั้น จะไม่ใช่ข้อมูลส่วนบุคคลตามกฎหมาย PDPA เพราะหากเป็นข้อมูลของบุคคลที่ประกอบกิจการในรูปบุคคลธรรมดา แล้วไปทำนิติกรรมใดใดโดยไม่จดทะเบียนนิติบุคคลแล้ว ข้อมูลของผู้ประกอบการคนเดียวที่ว่านั้นก็เป็นข้อมูลส่วนบุคคล

และที่สำคัญ บุคคลที่จะเป็นเจ้าของข้อมูลส่วนบุคคลได้นั้น จะต้องเป็น “สภาพเป็นบุคคลด้วย” หากตายไปแล้ว ก็ย่อมสิ้นสภาพของบุคคลไปตามที่กฎหมายกำหนดไว้ หรือกล่าวอย่างง่าย ๆ ก็คือบุคคลนอกเหนือจากจะไม่ใช่เป็นนิติบุคคลแล้ว จะต้องไม่ใช่คนตายที่หมดสภาพความเป็นบุคคลตามกฎหมายไปแล้วนั่นเอง

ข้อมูลส่วนบุคคล

(2)

**รูปแบบและประเภทของ
ข้อมูลส่วนบุคคล**

PDPA

Personal Data Protection Act

พระราชบัญญัติ

คุ้มครอง

ข้อมูลส่วนบุคคล

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

(1) ข้อมูลส่วนบุคคลแบบทั่วไป พุดอย่างรวบรัดได้เช่นที่กล่าวข้างต้นว่า ข้อมูลส่วนบุคคลแบบทั่วไปนั่นก็คือ ข้อมูลส่วนบุคคลแบบที่ไม่ได้เป็นข้อมูลอ่อนไหวตามมาตรา 26 ของกฎหมาย PDPA นั่นเอง โดยเป็นข้อมูลส่วนบุคคลที่มีหลักทั่วไปในการจัดเก็บรวบรวมตามที่มาตรา 24 กำหนด เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์มือถือ เป็นต้น

ข้อมูลส่วนบุคคล

(2) ข้อมูลส่วนบุคคลแบบอ่อนไหว (Sensitive Personal Data) 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 โดยตามกฎหมาย PDPA นั้นมีอยู่ 12 อย่างได้แก่

- 1) เชื้อชาติ
- 2) เผ่าพันธุ์
- 3) ความคิดเห็นทางการเมือง
- 4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- 5) พฤติกรรมทางเพศ
- 6) ประวัติอาชญากรรม
- 7) ข้อมูลสุขภาพ
- 8) ข้อมูลความพิการ
- 9) ข้อมูลสหภาพแรงงาน (ข้อมูลการเป็นสมาชิกสหภาพแรงงาน และข้อมูลอื่นที่เกี่ยวข้องกับการดำเนินงานของสหภาพแรงงาน เป็นต้น)

- 10) ข้อมูลพันธุกรรม
- 11) ข้อมูลชีวภาพ (Biometric Data เช่น ข้อมูลสแกนม่านตา ข้อมูลสแกนลายนิ้วมือ เป็นต้น)
- 12) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลที่จะประกาศต่อไป ซึ่งในอนาคตทางคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็อาจจะกำหนดให้ข้อมูลส่วนบุคคลบางรายการเช่น ประวัติการลงโทษทางวินัยของพนักงาน ข้อมูลค่าจ้าง เงินเดือน ค่าตอบแทนของพนักงาน เป็นข้อมูลอ่อนไหวเพิ่มเติมก็เป็นได้ อันนี้ก็ต้องรอฟังจากประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต่อไป

ข้อมูลส่วนบุคคล (Personal Data) นี้มีเยอะมาก มีทั้งข้อมูลส่วนบุคคลของพนักงาน ข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลส่วนบุคคลของคู่ค้า ซึ่งนับเป็นเรื่องที่เราจะต้องไปค้นหาให้ได้ว่ามีข้อมูลส่วนบุคคลของใคร เก็บไว้ที่ใดบ้างในฐานข้อมูล .oไฟล์ หรือระบบอะไรต่าง ๆ จากนั้นก็ต้องมากำหนดฐานการประมวลผลข้อมูลส่วนบุคคล (Data Processing Lawful Basis) และไปดำเนินการอื่นตามที่กฎหมายกำหนดไว้ต่อไป คราวนี้มาลองดูข้อมูลส่วนบุคคลของพนักงานหรือบุคลากรของเรา ก็มีหลากหลายอย่างมากไม่แพ้กัน ที่ว่ามันมีหลากหลายนั้นก็เพราะ

ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลหมายถึงข้อมูลสารสนเทศใด ที่นำมาใช้ระบุตัวตนของบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม ก็เข้าข่ายเป็นข้อมูลส่วนบุคคลทั้งนั้น เราได้ลองรวบรวมมาโดยแยกไว้ตามรูปแบบของข้อมูลเพื่อยืนยันว่ามันเจะจริง 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 รูปถ่าย เอกสารแสดงการเปลี่ยนชื่อ/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 ข้อมูลที่อยู่ของ

นักเรียนทุนที่เดินทางไปศึกษาต่อต่างประเทศ

3) ข้อมูลการศึกษา เช่น ท่านวุฒิการศึกษา ข้อมูลหลักฐานแสดงท่านวุฒิทางการศึกษา สถานศึกษา/สถาบัน สาขาวิชา วิชาเอก ปีที่สำเร็จการศึกษา คะแนนเฉลี่ยสะสม สำเนาใบแสดงผลการศึกษา สำเนาใบปริญญาบัตร หลักสูตรการฝึกอบรม/สัมมนาที่เกี่ยวข้อง ประกาศนียบัตร/ท่านวุฒิพิเศษ สถาบันที่มีการอบรมระยะเวลาอบรม ปีที่อบรม ข้อมูลเพื่อ ใช้บริหารจัดการด้านทุนการศึกษา ได้แก่ ผลการทดสอบที่ใช้สำหรับศึกษาต่อในประเทศ และต่างประเทศ 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 วันที่สิ้นสุดการ

ทำงาน อายุงาน) สถานภาพการจ้างงาน ผลการตรวจหาสารเสพติด ข้อมูลการตรวจสอบบุคคลอ้างอิง ข้อมูลหมายเลขประจำตัวผู้เสียภาษี ข้อเรียกร้อง ประกันภัยเงินทดแทนแรงงาน ประวัติการจ้างงาน วันที่เริ่มว่าจ้าง การเลิกจ้าง ทรัพย์สินที่อยู่ในความครอบครองระหว่างการจ้างงาน ข้อมูลการประเมินต่าง ๆ เช่นการประเมินผลการปฏิบัติงาน การประเมินสมรรถนะ เพื่อการวางแผนพัฒนาบุคลากรเป็นรายบุคคล เป็นต้น

5) ข้อมูลเกี่ยวกับเงินเดือนและสวัสดิการ เช่น บันทึกรายเงินเดือน (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 ข้อมูลเกี่ยวกับการตรวจสอบประวัติหมายเลขบัญชีที่มีกับสถาบันการเงิน ประวัติการทำธุรกรรมทางการเงิน ประวัติสินเชื่อ ข้อมูลการลงทุน เป็นต้น

ทั้งนี้ หากจะเจาะจงลงไปข้อมูลที่ส่วนบุคคลของพนักงานที่เป็นข้อมูลอ่อนไหว หรือ Sensitive Data ก็ได้แก่ (1) ข้อมูลสุขภาพ เช่น น้ำหนัก ส่วนสูง โรค

ประจำตัว โรคตาบอดสี ผลการตรวจร่างกาย ข้อมูลการ
 แพ้อาหาร ข้อมูลการแพ้ยา หมู่โลหิต ใบรับรองแพทย์
 ประวัติการรักษาพยาบาล ประวัติการรักษาพยาบาล
 (2) ข้อมูลชีวภาพ (Biometric Data) เช่น ข้อมูล
 จาลองลายนิ้วมือ ข้อมูลภาพจาลองใบหน้า เพื่อใช้ในการ
 ระบุดและยืนยันตัวตนของพนักงาน ป้องกันอาชญากรรม
 เป็นต้น (3) ข้อมูลเกี่ยวกับประวัติอาชญากรรม
 (Criminal Record) (4) ข้อมูลเกี่ยวกับความเชื่อใน
 ลัทธิศาสนา ปรัชญา (5) ข้อมูลเชื้อชาติ สัญชาติ
 (6) ข้อมูลความพิการของบุคคล อันมักจะปรากฏเป็น
 หนังสือรับรองผู้พิการ และบัตรประจำตัวผู้พิการ เป็นต้น
 (7) ข้อมูลการเป็นสมาชิกสหภาพแรงงาน รวมถึงการ
 ดำเนินกิจกรรมของสหภาพแรงงาน (8) ข้อมูล
 พันธุกรรม (Genetic Data) เป็นต้นครับ

ที่ว่ามานี้คงเป็นเพียงส่วนหนึ่งเท่านั้น แต่ไม่ว่าจะ
 มาก หรือไม่มากเพียงใดก็ตาม ก็ต้องหาให้พบทั้งหมด
 ซึ่งหลายองค์กรก็จะใช้ Software มาช่วยก็ได้ครับ

สำหรับเรื่องประเภทของข้อมูลส่วนบุคคลนั้น
 มีเขียนไว้ในกฎหมายอยู่แล้วครับ ลองไปดูในมาตรา 39 ก็
 จะเห็นว่ากฎหมายกำหนดให้เราละบุ้วัตถุประสงค์ของการ
 เก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท ซึ่งก็แปลว่า
 เราต้องมาจำแนกข้อมูลส่วนบุคคลที่เราทำการเก็บ
 รวบรวมไว้ให้ชัดเจนว่ามีที่ประเภทกันแน่ แต่หากจะตอบ
 ว่าข้อมูลส่วนบุคคลมีที่ประเภทนั้น ตอบยากครับ เพราะ

ข้อมูลส่วนบุคคล

แต่ละองค์กรก็กำหนดไม่เหมือนและไม่เท่ากัน

จากประสบการณ์ของเรา เราแนะนำให้องค์กรต่าง ๆ ทำการจำแนกประเภทของข้อมูลส่วนบุคคลที่องค์กรทำการจัดเก็บไว้เป็นประเภทต่าง ๆ รวม 13 ประเภทต่อไป นี้ ซึ่งท่านสามารถนำไปปรับใช้ได้ และในตอนท้ายเราจะให้ดูตัวอย่างว่า ลงข้อมูลตามประเภทของข้อมูลส่วนบุคคลอย่างไร ติดตามกันครับ

(1) ประเภทข้อมูลรายละเอียดส่วนบุคคล ได้แก่

- คำนำหน้านาม (นาย นาง นางสาว หม่อมหลวง)

- ยศ
- ชื่อ, ชื่อกลาง, นามสกุล, นามแฝง (หากมี)
- เพศ
- วันเดือนปีเกิด
- อายุ
- สถานภาพสมรส
- สถานภาพทางทหาร
- สัญชาติ

- ข้อมูลของคู่สมรส (เช่นชื่อ-นามสกุล ลายมือชื่อ)

- ข้อมูลของบุตร (เช่นชื่อ-นามสกุล อายุ)

- ข้อมูลของบิดา มารดา หรือบุคคลในครอบครัวอื่น

ข้อมูลส่วนบุคคล

(2) ประเภทข้อมูลเกี่ยวกับการติดต่อ ได้แก่

- ที่อยู่ติดต่อทางไปรษณีย์ เช่น บ้านเลขที่
- ที่อยู่อิเล็กทรอนิกส์ เช่น อีเมล แอดเดรส
- หมายเลขโทรศัพท์ที่ติดต่อมายังบุคคล (ไม่รวมบริษัท)
- หมายเลขโทรศัพท์มือถือ
- หมายเลขโทรสารส่วนบุคคล (ไม่รวมบริษัท)
- ชื่อตัวแทนหรือผู้มีอำนาจทำการแทนนิติบุคคล
- บัญชีสื่อสังคมออนไลน์ (social media)
- ข้อมูลโปรไฟล์อื่นสำหรับการสื่อสารทางอิเล็กทรอนิกส์

(3) ข้อมูลเกี่ยวกับการระบุและยืนยันตัวตน ได้แก่

- ภาพถ่ายบัตรประจำตัวประชาชน
- เลขประจำตัวประชาชน
- ข้อมูลหนังสือเดินทาง
- ใบอนุญาตขับรถยนต์
- ใบอนุญาตขับรถจักรยานยนต์
- ลายมือชื่อ หรือลายพิมพ์นิ้วมือ เพื่อเป็นหลักฐานยืนยันตัวบุคคล (ที่ไม่ใช่ข้อมูลชีวภาพ)
- หมายเลขประจำตัวผู้เสียภาษี (บุคคลธรรมดาเท่านั้น)
- ข้อมูลในทะเบียนบ้าน
- ภาพถ่ายหรือเคลื่อนไหวผ่านกล้อง CCTV
- ลักษณะรูปพรรณสัณฐานบุคคล
- บันทึกวิดีโอ หรือภาพเคลื่อนไหว

ข้อมูลส่วนบุคคล

(4) ประเภทข้อมูลเกี่ยวกับการทำงาน ได้แก่

- อาชีพ
- ตำแหน่งงาน
- หน้าที่งานที่รับผิดชอบในตำแหน่งงาน
- เงินเดือน หรือ รายได้
- ค่าตอบแทน
- เงิน หรือสิทธิประโยชน์ประจำตำแหน่ง
- โบนัส อัตราหรือจำนวนเงินโบนัส
- ใบผ่านงาน หรือใบผ่านการอบรม
- ใบรับรองหรือ Certificate การทำงาน
- สาขาความเชี่ยวชาญของผู้ปฏิบัติงาน
- ใบประกอบวิชาชีพ และเลขที่ใบประกอบวิชาชีพ เช่น ใบประกอบวิชาชีพทนายความ ใบประกอบโรคศิลปะ
- รายละเอียดเกี่ยวกับนายจ้างที่เคยผ่านงานหรือร่วมงาน
- สถานที่ทำงานล่าสุด หรือสถานที่ทำงานที่ผ่านมา
- หนังสือรับรองการฝึกอบรมเกี่ยวกับการทำงาน
- ผลการประเมินการปฏิบัติงาน (Performance)
- แผนการพัฒนาศักยภาพเป็นรายบุคคล
- ผลการประเมินศักยภาพหรือการพัฒนาบุคคล
- แผนและผลการปรับปรุงผลการปฏิบัติงาน (Performance Improvement Plan & Results)

ข้อมูลส่วนบุคคล

- ข้อมูลบุคคลอ้างอิงในประวัติการทำงาน
- ข้อมูลของบุคคลผู้ค้าประกัน
- รายละเอียดเกี่ยวกับนายจ้างที่เคยผ่านงานหรือร่วมงาน

• ข้อมูลจากผลการสำรวจพนักงาน เช่น ผลการสำรวจความเหนื่อยหน่ายในงาน ผลการสำรวจความรู้สึกผูกพันต่องานหรือต่อองค์กร ผลการสำรวจความพึงพอใจต่อการให้บริการของบุคลากร เป็นต้น

(5) ประเภทข้อมูลเกี่ยวกับการศึกษา ได้แก่

- วุฒิการศึกษา
- ผลการศึกษา
- วันเริ่มต้น-วันสำเร็จการศึกษา
- ชื่อสถาบันการศึกษาที่จบมา/กำลังศึกษา
- ชื่อสาขาวิชาที่สำเร็จการศึกษา/กำลังศึกษา
- ชื่อคุณวุฒิการศึกษาที่สำเร็จ/กำลังศึกษา

(6) ประเภทข้อมูลเกี่ยวกับการเงินและการติดต่อรับบริการ ได้แก่

- ผลิตภัณฑ์ และ/หรือ บริการต่าง ๆ ที่ใช้อยู่
- ช่องทางและวิธีการปฏิสัมพันธ์กับบริษัท
- สถานะความเป็นลูกค้าของท่าน
- ประวัติการชำระเงิน
- บันทึกการทำธุรกรรม
- ข้อมูลบัตรเครดิต และบัตรเดบิต
- รายรับและรายจ่าย
- กรณียสิินในบัญชี

ข้อมูลส่วนบุคคล

- รายละเอียดการชำระเงิน
- แหล่งที่มาของความมั่งคั่งและเงินทุน
- ประวัติการซื้อขายและยอดคงเหลือ
- ชื่อบัญชี หมายเลขบัญชี และประเภทบัญชี
- ประวัติบัญชีผู้ใช้
- กำไรและเงินลงทุน
- ข้อมูลการซื้อขาย เป็นต้น

(7) ประเภทข้อมูลเกี่ยวกับการวิจัยตลาด และการตลาดเรื่องอื่น ได้แก่

- การสำรวจความคิดเห็นลูกค้า
- ข้อมูลและความเห็นที่แสดงออกเมื่อเข้าร่วมวิจัยตลาด (เช่น คำตอบของท่านต่อคำถามแบบสอบถาม คำร้องขอทราบข้อเสนอแนะ และการทำวิจัย)
- รายละเอียดบริการที่ท่านได้รับและความต้องการของท่าน
- ข้อเสนอเกี่ยวกับท่านซึ่งอาจอิงจากการติดต่อระหว่างท่านกับบริษัท
- ข้อมูลการลงทะเบียนเพื่อรับข่าวสารเกี่ยวกับสินค้า
- ข้อมูลการลงทะเบียนเพื่อรับข่าวสารเกี่ยวกับบริการ
- ข้อมูลการลงทะเบียนสำหรับเข้าร่วมกิจกรรมทางการตลาด

(8) ประเภทข้อมูลเกี่ยวกับการใช้งานเว็บไซต์ ได้แก่

- หมายเลข IP Address ของคอมพิวเตอร์
- ข้อมูล Cookies
- ข้อมูลไอดีอุปกรณ์ (Device ID)
- ข้อมูลเบราว์เซอร์
- ข้อมูลการตั้งค่าเรื่องเขตเวลา (time zone)
- เว็บบีคอน (web beacon)
- ข้อมูลการเข้าถึง การเข้าสู่ระบบ (Login log) เช่นวันและเวลาที่เข้าถึง ระยะเวลาที่ใช้งาน เป็นต้น
- ข้อมูลการเข้าใช้งานแบบ single sign-on (SSO)
- ข้อมูลการตั้งค่าภาษา
- ข้อมูลการเข้าเว็บไซต์ และ Online Appointment System เป็นต้น

(9) ประเภทข้อมูลเกี่ยวกับการเข้าใช้งานระบบหรือ Application ได้แก่

- ข้อมูลการเข้าใช้ระบบของบริษัท
- ชื่อบัญชีผู้ใช้และรหัสผ่าน (Username และ Password)
- รหัสประจำตัว (PIN ID code)
- ข้อมูลกิจกรรมการใช้งานทางระบบ
- ข้อมูลกิจกรรมการใช้งานบน Application

(10) ประเภทข้อมูลอ่อนไหวอื่นที่ไม่ใช่ข้อมูลสุขภาพ (Non-health Data) ได้แก่

ข้อมูลส่วนบุคคล

- ศาสนา
- กรุ๊ปเลือด
- การเป็นสมาชิกพรรคการเมือง / ความคิดเห็นทางการเมือง
- ประวัติอาชญากรรม
- ข้อมูลความพิการ
- การเป็นสมาชิกสหภาพแรงงาน
- ข้อมูลเชื้อชาติ
- ข้อมูลชีวภาพ เช่น ข้อมูลสแกนลายนิ้วมือ สแกนใบหน้า สแกนรูม่านตา
- ข้อมูลเผ่าพันธุ์ หรือชาติพันธุ์ เช่น เผ่าอี้ก้อ เผ่ากะเหรี่ยง
- ข้อมูลความเชื่อในปรัชญาการเมือง เช่น ประชาธิปไตยนิยม

(11) ประเภทข้อมูลอ่อนไหวที่เป็นข้อมูลสุขภาพ (Health Data) ได้แก่

- ข้อมูลบริการด้านสุขภาพของผู้รับบริการ
- ข้อมูลที่เกี่ยวข้องกับการใช้ยา
- ข้อมูลที่เกี่ยวข้องกับการวินิจฉัยของแพทย์
- ข้อมูลการแพ้ยา แพ้อาหาร และ/หรือโรคประจำตัว
- ข้อมูลรายการยาตามใบที่แพทย์ได้สั่ง
- ข้อมูลส่วนสูง และน้ำหนัก ความดัน เพื่อการวินิจฉัยของแพทย์
- ข้อมูลอื่นที่จำเป็นต่อการให้คำปรึกษาติดตามอาการ
- ข้อมูลเกี่ยวกับการจำหน่ายยา/ผลิตภัณฑ์

ด้านสุขภาพอื่นๆ

- ข้อมูลห้องพักรักษาพยาบาล
- ข้อมูลผลการตรวจทางห้องปฏิบัติการ
- ข้อมูลผลการตรวจทางรังสีวินิจฉัย เป็นต้น

(12) ประเภทข้อมูลเกี่ยวกับการสื่อสารโต้ตอบ
ได้แก่

- บันทึกการโต้ตอบและการสื่อสารทางโทรศัพท์
- บันทึกการโต้ตอบและการสื่อสารทางอีเมล
- บันทึกการโต้ตอบและการสื่อสารทางหนังสือ
- ข้อมูลการสื่อสารทางสื่อสังคมออนไลน์ (Social Media) เป็นต้น

(13) ประเภทข้อมูลเกี่ยวกับกรรมสัมพันธ์
ได้แก่

- ข้อมูลเกี่ยวกับกรรมสัมพันธ์
- ผู้รับประกันภัย
- ผู้เอาประกันภัย
- ผู้รับประกันภัย
- หมายเลขกรรมสัมพันธ์
- ประเภทกรรมสัมพันธ์
- วงเงินคุ้มครอง
- ข้อมูลเกี่ยวกับการเคลมประกัน
- ข้อมูลเกี่ยวกับการเรียกร้องสินไหมทดแทน

ข้อมูลส่วนบุคคล

(3)

เจ้าของข้อมูลส่วนบุคคล

(Data Subject)

PDPA

Personal Data Protection Act

พระราชบัญญัติ

คุ้มครอง

ข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล (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

- บุคคลที่มีอายุตั้งแต่ 20 ปีบริบูรณ์ขึ้นไป หรือ
- ผู้ที่สมรสตั้งแต่อายุ 17 ปีบริบูรณ์ขึ้นไป หรือ
- ผู้ที่สมรสก่อนอายุ 17 ปี โดยศาลอนุญาตให้ทำการสมรส หรือ
- ผู้เยาว์ซึ่งผู้แทนโดยชอบธรรมให้ความยินยอมในการประกอบธุรกิจทางการค้าหรือธุรกิจอื่น หรือในการทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน ในความเกี่ยวข้องกับ

ข้อมูลส่วนบุคคล

การประกอบธุรกิจหรือ การจ้างแรงงาน
ข้างต้นให้ผู้เยาว์มีฐานะเสมือนดังบุคคลซึ่ง
บรรลุนิติภาวะแล้ว

ทั้งนี้ ในการให้ความยินยอมใด ๆ นั้น หาก
เจ้าของข้อมูลส่วนบุคคลเป็นผู้บรรลุนิติภาวะแล้ว ตาม
กฎหมายแล้ว เจ้าของข้อมูลส่วนบุคคลนั้นก็สามารถให้
ความยินยอมได้ด้วยตนเองได้โดยไม่ต้องผ่านบุคคลอื่น
เว้นแต่จะเป็นบุคคลที่บกพร่องเรื่องความสามารถตามที่
กฎหมายกำหนด เช่น บุคคลไร้ความสามารถ หรือบุคคล
เสมือนไร้ความสามารถ ซึ่งจะไม่ลงรายละเอียดกล่าวถึง
ในเนื้อหาเล่มนี้แต่อย่างใดครับ

(2) เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ คือบุคคล
ที่อายุต่ำกว่า 20 ปีบริบูรณ์ และไม่ใช่ผู้บรรลุนิติภาวะตาม
ข้อ 1) โดยในการให้ความยินยอมใด ๆ จะต้องได้รับความ
ยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทน
ผู้เยาว์ด้วย

(3) เจ้าของข้อมูลส่วนบุคคลที่เป็นคนเสมือนไร้
ความสามารถ หรือบุคคลที่ศาลสั่งให้เป็นคนเสมือนไร้
ความสามารถ เนื่องจากมีกายพิการหรือมีจิตฟั่นเฟือนไม่
สมประกอบ หรือประพฤตีสຸ່ຍສຸ່ຍສະເພາະเป็นอาชญา
หรือติดสุรายาเมา หรือมีเหตุอื่นใดทำนองเดียวกันนั้น จน
ไม่สามารถจะจัดทำกรงานโดยตนเองได้ หรือจัดกิจการ
ไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือ
ครอบครัว ในการให้ความยินยอมใด ๆ จะต้องได้รับ

ข้อมูลส่วนบุคคล

ความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคน
เสมือนไร้ความสามารถนั้นก่อน

(4) เจ้าของข้อมูลส่วนบุคคลที่เป็นคนไร้
ความสามารถ หรือเป็นบุคคลที่ศาลสั่งให้เป็นคนไร้
ความสามารถ เนื่องจากเป็นบุคคลวิกลจริต ทั้งนี้ ใน
การให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจาก
ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถนั้น
ก่อน

ทั้งนี้ มีหลักทางกฎหมายที่ท่านจะต้องไม่ลืมเลยก็
คือหลักที่ว่าหากการขอความยินยอมจากเจ้าของข้อมูล
ส่วนบุคคลที่ไม่เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล การให้ความยินยอมนั้นก็จะมีผลผูกพันเจ้าของ
ข้อมูลส่วนบุคคล เนื่องจากเป็นการให้ความยินยอมที่
ไม่ชอบด้วยกฎหมายซึ่งกฎหมายไม่รับรองครับ

และเมื่อพูดถึงเจ้าของข้อมูลส่วนบุคคลแล้ว ก็ต้อง
ไปพูดถึงต่อถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งขอ
กล่าวไว้ย่อ ๆ ก่อนที่จะลงไปรายละเอียดในหัวข้อที่
เกี่ยวข้องอีกครั้ง กล่าวคือ เจ้าของข้อมูลส่วนบุคคลนั้น
มีสิทธิ 9 อย่างได้แก่ (1) สิทธิในการเพิกถอนความ
ยินยอม (Right to withdraw consent) (2) สิทธิใน
การเข้าถึงข้อมูลส่วนบุคคล (Right of access) (3)
สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to
rectification) (4) สิทธิในการลบข้อมูลส่วนบุคคล
(Right to erasure) (5) สิทธิในการระงับการใช้ข้อมูล

ข้อมูลส่วนบุคคล

ส่วนบุคคล (Right to restriction of processing) (6) สิทธิในการให้ออนย้ายข้อมูลส่วนบุคคล (Right to data portability) (7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to object) และ (8) สิทธิในการได้รับแจ้งข้อมูลให้ทราบ (Right to be informed) และ (9) สิทธิในการร้องเรียนเรื่องการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งท่านจำเป็นต้องจัดทำระบบการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ครับ โดยจะไปว่าไว้ในเนื้อหาส่วนที่เป็น 8 ขั้นตอนของการทำ PDPA Implementation ต่อไป

PDPA

Personal Data Protection Act

พระราชบัญญัติ
คุ้มครอง
ข้อมูลส่วนบุคคล