

150 คำถาม-คำตอบ

PDPA

รวมประเด็นน่ารู้เกี่ยวกับ
กฎหมายคุ้มครองข้อมูลส่วนบุคคล
แบบ Q&A ที่หลายท่านคาใจ



เคลียร์ทุกข้อสงสัย พร้อมอธิบายให้เข้าใจชัดเจน

ดร.ชัชวาล อรวงศ์ศุกทัต
ทนายฝ่าย ยิงพร อินทร์ศรีชื่น
วิทยากรและที่ปรึกษา PDPA

150

คำถาม-คำตอบ

PDPA

ัชชวาล อรวงศ์สุภักต
ย้งพร อินทร์ศรีชั้น

วิทยากรและที่ปรึกษา PDPA

150 คำถาม-คำตอบ PDPA

รวมประเด็นน่ารู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลแบบ
Q&A ที่หลายท่านคาใจ

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ

ัชชวาล อรวงศ์ศุภกัต
และย้งพร อินทร์ศรีชั้น

150 คำถาม-คำตอบ PDPA.

กรุงเทพฯ : Professional Training and Consultancy, 2564

ISBN : 978-616-586-847-1

สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537

ห้ามลอกเลียนแบบไม่ว่าส่วนหนึ่งส่วนใดของหนังสือเล่มนี้

ไม่ว่ารูปแบบใดๆ นอกจากจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้เขียนเท่านั้น

บรรณาธิการ : ชัชวาล อรวงศ์ศุภกัต และย้งพร อินทร์ศรีชั้น

จัดพิมพ์โดย : ชัชวาล อรวงศ์ศุภกัต และย้งพร อินทร์ศรีชั้น

ออกแบบปกโดย : ย้งพร อินทร์ศรีชั้น

รูปเล่ม : ย้งพร อินทร์ศรีชั้น

พิสูจน์อักษร : สุราสินี ถึงแสง

จัดทำเล่ม : บริษัท Professional Training and Consultancy จำกัด
142/129 หมู่ที่ 5 ถนนสวนผัก 32 ตำบลมหาสวัสดิ์
อำเภอบางกรวย จังหวัดนนทบุรี 11130

ติดต่อฝึกอบรมหรืองานที่ปรึกษาได้ที่

อีเมล : ptccontactt@gmail.com

โทรศัพท์ : 089-677-6047, 092-431-6631

จำนวนหน้า : 400 หน้า

ราคา : 429 บาท

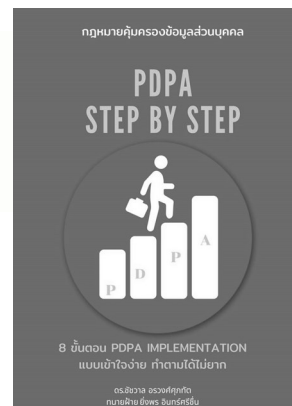
ความนำ

150 คำถาม-คำตอบ PDPA

หลังจากที่เราได้จัดพิมพ์หนังสือ 108-1009 คำถาม PDPA ไปแล้วสองเล่ม เล่มแรกเป็นรวมคำถาม-คำตอบ PDPA เรื่องทั่วไป มีความหนาประมาณ 150 หน้า และเล่มสอง เป็นคำถาม-ตอบ PDPA ที่เน้นไปในงาน HR ทั้ง 6 ด้านและเน้นในด้านงานสรรหาและคัดเลือกบุคลากรเป็นหลัก ความหนาประมาณ 250 หน้า ปรากฏว่าหนังสือแต่ละเล่มของเราหมดภายในเวลาอันรวดเร็ว ซึ่งคงเป็นด้วยจำนวนเล่มที่จัดพิมพ์ออกมาในจำนวนเพียงเล็กน้อยเท่านั้น และก็มี Demand ของท่านผู้อ่านอีกจำนวนหนึ่ง อันเป็นที่มาของการเรียบเรียงหนังสือเล่มนี้

และที่สำคัญนั้น เพื่อให้ประหยัต์กับท่านทั้งหลาย ในสภาพเศรษฐกิจที่ไม่ค่อยสวยงามนักเช่นปัจจุบัน เราจึงตัดสินใจรวมเล่มหนังสือสองเล่มที่กล่าวถึงข้างต้นของเรา และปรับปรุงเนื้อหาใหม่ โดยเพิ่มคำถาม-ตอบอีกหลายเรื่องที่น่าสนใจเข้าไป ออกมาให้เป็นเล่มที่ท่านกำลังถือในมือนี้ ในรูปแบบ e-book ซึ่งก็ตอบเป้าหมายเรื่องการประหยัต์ทั้งเราและท่านได้แน่นอนว่าต้นทุนที่ลดลง มันทำให้เราสามารถตั้งราคาจำหน่ายได้ต่ำลงไปมากนั่นเอง

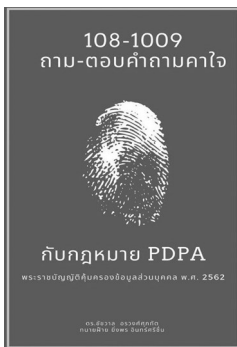
ด้วยความที่หนังสือเกี่ยวกับ PDPA ในบ้านเราตอนนี้ มีไม่กี่เล่มสองเล่มในมีที่เล่มนั้นเป็นหนังสือวิชาการที่เขียนโดยนักวิชาการและนักกฎหมาย และนอกจากผู้เชี่ยวชาญด้าน PDPA อีกบางท่านที่เขียนหนังสือแนวนี้ออกมาแล้ว ก็คงมีอีกสามปวกที่เราจัดพิมพ์ออกมาเป็นเล่มแล้ว สองเล่มแรกนั้น เราทำเป็นแนวคำถาม-ตอบ ส่วนเล่มที่ 3 นั้นเป็นแนวแนะนำพื้นฐานความรู้เกี่ยวกับ PDPA และแนะนำขั้นตอนการ Implement PDPA ในองค์กร (ตามภาพ) เราคิดว่า ท่านจะได้ประโยชน์อย่างมากจากหนังสือของเรา



ความนำ

150 คำถาม-คำตอบ PDPA

เพื่อสนองความต้องการของเราในการแนะนำความรู้เชิงการถาม-ตอบให้แก่ท่านที่อาจจะไม่ได้ติดตามเล่มที่ 1 และเล่มที่ 2 ที่เราได้กล่าวถึงไปข้างต้น ประกอบกับหนังสือเล่มก็หมดไปเรียบร้อย เราจึงได้ทำรวมเล่มออกมาเป็น “150 คำถาม-คำตอบ PDPA” ในรูปแบบ e-book นี้



และที่ใคร่ขอฝากคุณผู้อ่านติดตามผลงานของเราต่อไป รับรองว่าได้ประโยชน์อย่างแน่นอน เพราะเราตั้งใจเรียบเรียงคำตอบออกมาให้เห็นทั้งแง่มุมทางกฎหมาย ที่ต้องเข้าใจมันให้ดี และแง่มุมการบริหารจัดการจากประสบการณ์ของเราทั้งสองคนที่ต่างเชี่ยวชาญแต่ละแง่มุม (กฎหมายและการบริหารจัดการ) ทั้งจากประสบการณ์การเป็นวิทยากร และการให้คำปรึกษาในหลายองค์กร เราจึงเชื่อว่าเนื้อหาใน e-book นี้ จะเป็นอีกส่วนหนึ่งที่ช่วยให้คุณผู้อ่านนำไปใช้ประโยชน์กับการ Implement PDPA ในองค์กรของท่านทั้งหลายได้มากขึ้น สมเจตนาของเราผู้เขียน

ด้วยความเชื่อมั่นว่าท่านจะได้นำสิ่งที่ได้เรียนรู้จากเราไปใช้ประโยชน์

อาจารย์ ดร.ชัชวาล อรวงศ์ศุภกิต
หนายความ ยิงพร อินทร์ศรีชั้น
ตุลาคม 2564

สารบัญ

150 คำถาม-คำตอบ PDPA

(1) กฎหมาย PDPA คืออะไร ?	1
(2) ประเทศอื่นเขามีกฎหมาย PDPA เหมือนประเทศไทยหรือไม่ ?	1
(3) กฎหมาย PDPA สำคัญกับองค์กรอย่างไร ?	4
(4) ข้อมูลส่วนบุคคล (Personal Data) คืออะไร ?	7
(5) ข้อมูลส่วนบุคคลมีกี่แบบ ?	9
(6) ข้อมูลส่วนบุคคล (Personal Data) ของลูกค้าและคู่ค้ามีอะไรบ้าง ?	13
(7) ข้อมูลส่วนบุคคลของพนักงาน (Employee Personal Data) มีอะไรบ้าง ?	14
(8) หากจะสอบถามข้อมูลของผู้สมัครงานจากบุคคลอ้างอิง (Reference Person) ต้องทำอย่างไรจึงจะสอดคล้องกับกฎหมาย PDPA ?	20
(8) ข้อมูลส่วนบุคคลของผู้สมัครงานมีอะไรบ้าง ?	22
9) เมื่อมีผู้สมัครงานส่ง Resume เข้ามาสมัครงานทางอีเมล เราจะต้องทำอย่างไรกับข้อมูลส่วนบุคคลของผู้สมัครงานนั้น ?	22
(10) ทำอย่างไรกับกรณี HR ขององค์กรอื่นโทรมาสอบถามข้อมูลเกี่ยวกับการทำงานของพนักงาน ?	23
(11) เมื่อมีพนักงานของสถาบันการเงินติดต่อเข้ามาขอยืนยันข้อมูลพนักงานเนื่องจากพนักงานไปขอกู้สินเชื่อ เราจะเปิดเผยข้อมูลนั้นได้มั้ย ต้องขอความยินยอมพนักงานก่อนหรือไม่ ?	26

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

(12) ทำอย่างไรเมื่อบุคคลภายนอกสอบถามข้อมูลเกี่ยวกับพนักงานของเรา จึงจะไม่ผิดกฎหมาย ?	28
(13) การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงานหรือพนักงานในเรื่องใดบ้างที่ต้องขอความยินยอม ?	39
(14) ใครกันที่ควรจะต้องรับหน้าที่จัดการกับการใช้สิทธิ ของเจ้าของข้อมูลส่วนบุคคล ?	40
(15) กิจกรรมและใครบ้างที่ไม่ต้องปฏิบัติตามกฎหมาย PDPA ?	42
(16) กิจกรรมส่วนบุคคลหรือกิจกรรมเพื่อประโยชน์ส่วนตนเป็นอย่างไร ได้แก่อะไรบ้าง ?	44
(17) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐที่ไม่ต้องปฏิบัติตามกฎหมาย PDPA นั้น มีหน่วยงานประมาณใด ?	44
(18) กฎหมาย PDPA บังคับใช้กับคนไทยและในประเทศไทยเท่านั้น ใช่หรือไม่ ?	45
(19) เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือใคร ?	46
(20) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือใคร และมีหน้าที่อะไรบ้าง ?	49
(21) มีหลักการหรือแนวทางการพิจารณาว่าองค์กรมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	52
(22) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือใครและมีหน้าที่อย่างไรบ้าง ?	54

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

(23) มีหลักการหรือแนวทางการพิจารณาว่าองค์กรมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) อย่างไรบ้าง ?	57
(24) Data Protection Officer คือใคร และต้องมีคุณสมบัติอย่างไรบ้าง ?	58
(25) องค์กรหรือหน่วยงานใดที่จะต้องแต่งตั้ง Data Protection Officer บ้าง ?	60
(26) Data Protection Officer มีหน้าที่อะไรบ้าง ?	62
(27) ถ้าจะต้องแต่งตั้ง Data Protection Officer ขึ้นมา จะต้องทำอย่างไรดี ?	64
(28) เขียนหน้าที่ DPO ในคำสั่งแต่งตั้งอย่างไรดี ?	66
(29) ถ้าองค์กรไม่สนับสนุนการทำงานของ DPO จะมีปัญหาอย่างไรบ้าง ?	67
(30) จะตั้งพนักงานสักคนหนึ่งมาเป็น DPO หรือจะว่าจ้างองค์กรภายนอกที่เค้ามีประสบการณ์ให้มาเป็น DPO ให้กับองค์กรของเรา แบบใดดีกว่ากัน ?	69
(31) การประมวลผลข้อมูลส่วนบุคคลคืออะไร ?	70
(32) ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูล ต้องทำข้อตกลงหรือสัญญาอะไรกับองค์กรของเรา (เราเป็นผู้ควบคุมข้อมูลส่วนบุคคล) ?	72
(33) ตามกฎหมาย PDPA มีหลักการในการเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลกำหนดไว้อย่างไรบ้าง ?	74

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (34) บริษัทของเรากำหนดให้ตรวจสอบประวัติอาชญากรรมจาก
ผู้สมัครงานก่อนตัดสินใจคัดเลือกเข้าร่วมงาน อยากรู้
คำแนะนำว่าจะเก็บรวบรวมข้อมูลอย่างไร ? **77**
- (35) องค์กรหนึ่งใด อาจเป็นทั้งผู้ควบคุมข้อมูล และ
อาจจะเป็นผู้ประมวลผลข้อมูลไปพร้อมกันก็ได้
ใช่หรือไม่ ? **80**
- (36) องค์กรมอบหมายงานให้พนักงานบางตำแหน่งเช่น
พนักงาน HR จะต้องเก็บรวบรวม ใช้หรือเปิดเผย
ข้อมูลส่วนบุคคลของพนักงานคนอื่น แบบนี้ เราต้อง
ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับ
พนักงานหรือไม่ ? **80**
- (37) มีหลักการเก็บรวบรวมข้อมูลจากบุคคลหรือนิติบุคคล
อื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลอย่างไรบ้าง ? **82**
- (38) รปภ.ต้องเก็บข้อมูลส่วนบุคคลจากผู้มาติดต่อ ลูกค้า
หรือพนักงาน แล้วจะจัดการอย่างไรเพื่อให้เป็นไปตาม
กฎหมาย ? **84**
- (39) มีคำแนะนำเกี่ยวกับการใช้และเปิดเผยข้อมูลส่วนบุคคล
ให้เป็นไปตามกฎหมาย PDPA อย่างไรบ้าง ? **85**
- (40) การขอความยินยอม (Consent) กับเจ้าของข้อมูล
ส่วนบุคคลนั้น มีหลักการอย่างไรบ้าง ? **87**
- (41) หากไม่ต้องการที่จะขอความยินยอมกับเจ้าของข้อมูล
ส่วนบุคคลกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูล
ส่วนบุคคลแบบทั่วไป จะทำอย่างไรได้บ้าง ? **88**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

(42) ทำไมจึงควรหลีกเลี่ยงการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ?	90
(43) ฐานการประมวลผลข้อมูลส่วนบุคคลคืออะไร ?	92
(44) ฐานการประมวลผลข้อมูลส่วนบุคคล ตามกฎหมาย PDPA มีกี่แบบ ?	92
(45) 6 ฐานการประมวลผลข้อมูล (Lawful Basis) โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล สำหรับข้อมูลแบบทั่วไปนั้น มีตัวอย่างในเรื่องใดบ้าง ?	93
(46) มีแนวทางการใช้ฐานความยินยอมกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างไร บ้าง เพื่อให้ไม่มีปัญหาไม่ทำตามกฎหมาย ?	99
(47) ฐานสัญญา (Contract) ใช้ในกรณีใดบ้าง ?	101
(48) ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) ใช้อย่างไร และมีตัวอย่างเรื่องใดบ้าง ?	103
(49) จะใช้ฐานระงับอันตรายต่อชีวิต ร่างกายและสุขภาพ (Vital Interest) กับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลอ่อนไหวอย่างไรดี ?	104
(50) จะใช้ฐานภารกิจสาธารณะ (Public Task) กับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแบบทั่วไปอย่างไรดี ?	105
(51) จะใช้ฐานประโยชน์อันชอบธรรม (Legitimate Interest) กับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างไรดี ?	106

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

(52) มีหลักการอย่างไรในการพิจารณาว่ากิจกรรมงานนั้นเหมาะสมหรือสามารถเลือกใช้ฐานประโยชน์อันชอบธรรมได้ ?	107
(53) หลักการ 3 Test ที่อธิบายกัน โดยเฉพาะในเอกสารแนะนำความรู้เรื่อง PDPA ของตลาดหลักทรัพย์แห่งประเทศไทยนั้น มีสาระอย่างไรบ้าง ?	108
(54) มีตัวอย่างการพิจารณาตามหลักทดสอบสามอย่างหรือหลัก 3 Test อย่างไรบ้าง ?	110
(55) มีตัวอย่างของกิจกรรมงานใดบ้าง ที่สามารถเลือกใช้ฐานประโยชน์อันชอบธรรมหรือฐานประโยชน์โดยชอบด้วยกฎหมาย มาปรับใช้ ?	111
(56) ภาพถ่ายและวิดีโอบุคคล ลักษณะใดบ้างที่ไม่ต้อง “ขอความยินยอม (Consent)” ?	112
(57) ต้องขอความยินยอมจากการใช้สำเนาสำเนาบัตรประชาชนของผู้บริหารระดับสูงที่จะนำไปใช้ประกอบการเข้าซื้อเครื่องถ่ายเอกสารของบริษัทหรือไม่ ?	113
(58) ทำอย่างไรจึงจะไม่ต้องยุ่งยากกับการขอความยินยอมการประมวลผลข้อมูลส่วนบุคคลจากผู้สมัครงาน ?	115
(59) ทำไมต้องขอความยินยอมตรวจสอบประวัติอาชญากรรมจากผู้สมัครงาน ?	118
(60) จะสามารถอ้างประโยชน์อันชอบธรรม (Legitimate Interest) ขององค์กรกับการสรรหาว่าจ้างผู้สมัครเข้าร่วมงานได้หรือไม่ ?	120

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- 61) จะสามารถอ้างฐานการปฏิบัติตามสัญญา (Contract) กับการเก็บรวบรวมข้อมูลประวัติส่วนบุคคลของผู้สมัครงานในตำแหน่งงานที่เราเปิดรับสมัครได้หรือไม่ ทั้งนี้ องค์กรยังไม่ได้ทำสัญญาจ้างแต่อย่างใด ? **121**
- (62) จะเขียนข้อความใน Privacy Notice เพื่ออ้างประโยชน์อันชอบธรรม (Legitimate Interest) กับการสรรหาว่าจ้างผู้สมัครเข้าร่วมงานประมาณใดดี ? **124**
- (63) หากจะสอบถามข้อมูลของผู้สมัครงานจากบุคคลอ้างอิง (Reference Person) ต้องทำอย่างไร จึงจะสอดคล้องกับกฎหมาย PDPA ? **134**
- (64) ว่าจ้าง Recruitment Agency ส่งผู้สมัครงานระดับ Manager มาให้เราสัมภาษณ์และคัดเลือกคนที่เหมาะสมเข้าทำงาน จะต้องทำอะไรบ้างกับ Recruitment Agency จึงจะไม่มีปัญหาผิดกฎหมาย PDPA ? **136**
- (65) ประวัติส่วนบุคคลของผู้สมัครงานที่ไม่ผ่านการพิจารณา เราจะเก็บไว้นานเท่าใด จะได้ไม่เป็นภาระขององค์กร ? **138**
- (66) ใช้ข้อมูลประวัติส่วนบุคคลของผู้สมัครงานเพื่อวัตถุประสงค์ในการสรรหาคัดเลือก เมื่อผ่านการพิจารณาแล้วจะต้องมาทำสัญญาว่าจ้าง จะใช้ข้อมูลนั้นต่อไปได้หรือไม่ ? **139**
- (67) ผู้เชี่ยวชาญต่างบอกไปในทางเดียวกันว่า ให้เก็บรวบรวมข้อมูลของผู้สมัครงานเท่าที่จำเป็น แต่แค่ไหนคือเท่าที่จำเป็น ? **140**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- | | |
|---|-----|
| (68) ควรปรับปรุงการรับสมัครงานอย่างไรให้ ไม่เสี่ยงกับ
ผิดกฎหมาย PDPA ขอคำแนะนำและตัวอย่าง ? | 141 |
| (69) บริษัทของเรา อาจต้องส่งข้อมูลพนักงาน หรือข้อมูล
ลูกค้าให้กับบริษัทแม่ที่ต่างประเทศ เราต้องทำอะไรบ้าง
กับกรณีนี้ เพื่อให้สอดคล้องกับกฎหมายPDPA ? | 148 |
| (70) ใช้ประวัติส่วนบุคคลของวิทยากรภายนอกที่ว่าจ้างเข้ามา
จัด In-house Training ต้องขอความยินยอมจาก
วิทยากรหรือไม่ ? | 152 |
| (71) จะอ้างฐานการประมวลผลข้อมูลฐานใดกับการเก็บรวบรวม
ใช้และเปิดเผยข้อมูลส่วนบุคคลสำหรับการฝึกอบรม
พนักงาน ? | 154 |
| (72) ในงานฝึกอบรมและพัฒนาบุคลากร โดยทั่วไปจะ
อ้างอิงฐานการประมวลผลข้อมูลส่วนบุคคลบ้าง
และต้องเขียนวัตถุประสงค์ไว้เช่นใดบ้าง ? | 156 |
| (73) เมื่อฝึกอบรมเสร็จ ต้องให้พนักงานทำแบบสำรวจความ
พึงพอใจต่อการจัดฝึกอบรมแต่ละครั้งต้อง
ขอความยินยอมจากพนักงานก่อนเก็บข้อมูลหรือไม่ ? | 157 |
| (74) เมื่อส่งพนักงานไปเข้ารับการอบรมกับองค์กรภายนอก
(Public Training) เราต้องทำ Data Processing
Agreement (DPA) หรือข้อตกลงการประมวลผล
ข้อมูลส่วนบุคคลกับบริษัทให้บริการฝึกอบรมหรือไม่ ? | 158 |
| (75) ควรทำ Privacy Notice เรื่องการฝึกอบรมพนักงาน
แล้วให้พนักงานลงชื่อรับทราบไว้หน้าห้องฝึกอบรม
ทุกครั้งหรือไม่ ? | 161 |

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (76) ข้อมูลผลการประเมินการปฏิบัติงานรอบกลางปีและรอบปลายปี ที่ระบุผลการดำเนินงานต่ำกว่าเป้าหมายเป็น Sensitive Data หรือไม่ ? **165**
- (77) หัวหน้าประเมินผลงานของพนักงานที่เป็นลูกน้องของตัวเอง จะต้องขอความยินยอมการประมวลผลข้อมูลจากพนักงานหรือไม่ ถ้าจะต้องขอ HR หรือหัวหน้าควรเป็นฝ่ายที่จัดการเรื่องนี้ ? **167**
- (78) HR ที่ทำงาน Payroll จะต้องทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับบริษัทหรือไม่ ? **168**
- (79) บริษัทมีสวัสดิการเป็นบัตรประกันสุขภาพให้พนักงาน โดยใครไปรักษาตัวแล้วสำรองจ่ายไปก่อน ก็เอาใบเสร็จมาเบิกคืนได้ กรณีนี้ ต้องขอความยินยอมจากพนักงานทุกครั้งหรือไม่ ? **170**
- (80) บริษัทมีสวัสดิการทุนเล่าเรียนบุตรของพนักงานที่เรียนดี มอบให้ทุกปี แต่จะต้องใช้ข้อมูลผลการเรียนของบุตรพนักงานมาประกอบ แบบนี้ จะต้องทำอย่างไรจึงจะสอดคล้องกับกฎหมาย PDPA ? **171**
- (81) HR ออกหนังสือส่งตัวผู้สมัครงานไปตรวจสุขภาพก่อนเริ่มงาน ต้องไปทำเรื่องขอความยินยอมจากผู้สมัครงานหรือไม่ ? **173**
- (82) HR ต้องส่งข้อมูลการเสียภาษีไปยังกรมสรรพากร จะอ้างฐานใดเพื่อการนำส่ง และเอกสารนี้ ควรจัดเก็บไว้ยาวนานเพียงใด ? **174**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (83) ถ่ายภาพและอัดวีดีโอพนักงานระหว่างทำกิจกรรมของบริษัท โดยที่องค์กรไม่ขอความยินยอมจากพนักงานจะผิดกฎหมายหรือไม่ ? **177**
- (84) ต้องระมัดระวังการเปิดเผยข้อมูลส่วนบุคคลอย่างไรบ้าง เมื่อต้องสอบสวนพนักงานที่ต้องขอล่าว่าหาว่ากระทำ “ผิดวินัย” ? **177**
- (85) HR ได้รับมอบหมายจากบริษัทให้ทำสำรวจความผูกพันต่อองค์กรหรือ Employee Engagement Survey (EES) ทุกเดือนตามแบบสำรวจที่เราซื้อมาจากองค์กรภายนอก การเก็บข้อมูลแต่ละครั้ง ต้องทำอย่างไรจึงจะสอดคล้องกับกฎหมาย PDPA ? **178**
- (86) จะเปิดเผยข้อมูลการเป็นสมาชิกสหภาพแรงงานของพนักงานให้หัวหน้างานทราบไว้ เพื่อรู้ว่าลูกน้องของตัวเองคนใดเป็นสมาชิกของสหภาพแรงงานบ้าง ต้องขอความยินยอมพนักงานหรือไม่ ? **178**
- (87) จะต้องจัดการอย่างไรกับกล้อง CCTV ที่ติดไว้ลานจอดรถหรือพื้นที่ภายในอาคารอย่างไร ? **180**
- (88) จัดการกับจดหมาย พัสดุไปรษณีย์ของพนักงานที่ Admin รับไว้จากผู้ส่งอย่างไรดี จะได้ไม่มีปัญหาตามกฎหมาย PDPA ? **181**
- (89) หากไม่ต้องการที่จะขอความยินยอมกับเจ้าของข้อมูลส่วนบุคคลกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลแบบอ่อนไหว จะทำอย่างไรได้บ้าง ? **182**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

(90) 10 ฐานของการประมวลผลข้อมูลส่วนบุคคลแบบอ่อนไหวคืออะไรและมีอะไรบ้าง ?	184
(91) ความยินยอมโดยชัดแจ้ง (Explicit Consent) ที่เป็นฐานการประมวลผลข้อมูลส่วนบุคคลแบบอ่อนไหวนั้นมีแนวทางปรับใช้อย่างไร ?	186
(92) การอ้างความจำเป็นเพื่อการปฏิบัติตามกฎหมายเกี่ยวกับการให้บริการด้านสุขภาพหรือสังคม ตามมาตรา 26 (5) (ก) และการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข ตามมาตรา 26 (5) (ข) ที่จะไม่ต้องไปขอความยินยอมในการประมวลผลข้อมูลแบบอ่อนไหวจากเจ้าของข้อมูลส่วนบุคคลนั้น เกี่ยวกับเรื่องอะไรบ้าง ?	187
(93) HR จะต้องเกี่ยวข้องกับการปฏิบัติตามกฎหมายเกี่ยวกับการคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ ซึ่งเป็นหนึ่งในฐานการประมวลผลข้อมูลแบบอ่อนไหวอย่างมาก ในฐานนี้ว่าไว้อย่างไรบ้าง ?	190
(94) เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของเราได้หรือไม่ ?	191
(95) เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ลบทำลายข้อมูลของเขาในเรื่องใดได้บ้าง ?	192
(96) ควรทำแบบฟอร์มให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิเพิกถอนความยินยอมแต่ละกรณี ๆ ด้มัย ?	194
(97) หากจะทำแบบฟอร์มให้เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิตามกฎหมาย PDPA บนเว็บก็ได้หรือไม่หรือไม่ ?	198

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- | | |
|--|-----|
| (98) ดูจากกฎหมายแล้วตีความได้ว่า ไม่ว่าจะพนักงาน ลูกค้าหรือผู้สมัครงาน ก็สามารถขอรับสำเนาข้อมูลส่วนบุคคลของเขาจากเราได้ แล้วเราควรทำอะไรบ้างรองรับเรื่องนี้ ? | 200 |
| (99) การเก็บรวบรวมข้อมูลส่วนบุคคลตามกฎหมาย PDPA นั้น องค์กรต้องแจ้งเรื่องใดบ้างให้เจ้าของข้อมูลส่วนบุคคลทราบ ? | 202 |
| (100) ตามกฎหมาย PDPA เหตุใดต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลส่วนบุคคลทราบ ? | 204 |
| (101) บริษัทได้ทำสัญญาจ้างบริษัทรักษาความปลอดภัยใหม่ แต่ในสัญญาที่ทำไว้แล้ว ยังไม่มีรายละเอียดเกี่ยวกับ PDPA เราสามารถ ทำสัญญาแนบเกี่ยวกับการ Consent ได้หรือไม่ ? | 205 |
| (102) เข้าไปสั่งไก่ทอด KFC หรือเข้าแอฟริกาตามตัวอย่างนี้ เจ้าแจ้งอะไรมาให้เรากันนะ ? | 206 |
| (103) ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ควรต้องเขียนเรื่องอะไรไว้บ้าง ? | 207 |
| (104) เราจะทำอย่างไรดี เพราะกฎหมายกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่อยู่กับองค์กรของเรา ? | 208 |
| (105) อาจารย์เคยคุยใน Podcast Practical PDPA ว่า กฎหมาย PDPA นี้จะเปลี่ยนแปลงงานที่ทางองค์กรต้องจัดการ สปท.ที่ว่าจ้าง ไปอย่างมาก มันจะเปลี่ยนไปอย่างไรบ้าง ? | 210 |

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (106) จำเป็นต้องเก็บข้อมูลส่วนบุคคลของบิดา มารดา บุคคลในครอบครัวของผู้สมัครงานหรือไม่ ? **212**
- (107) จำเป็นต้องเก็บข้อมูลส่วนบุคคลของผู้สมัครงานในเรื่องตามตัวอย่างเหล่านี้หรือไม่ ถ้าองค์กรก็อยากเก็บ จะต้องทำอย่างไร และมีตัวอย่างหรือไม่ ? **213**
- (108) ข้อมูลส่วนบุคคลของพนักงานบางอย่างที่เราเก็บรวบรวมไว้ แล้วเราอยากจะจัดการมันเหมือนกับเป็น Sensitive Data แต่ตามกฎหมายมันไม่ได้เป็น Sensitive Data จะสามารถทำได้หรือไม่ ? **217**
- (109) ในสัญญาจ้างที่ใช้ในปัจจุบัน จะกำหนดให้ทุกคนที่เป็นพนักงานใหม่จะต้องตรวจสอบสุขภาพและหากมีผลการตรวจสุขภาพไม่ผ่านตามเกณฑ์ที่องค์กรกำหนด ซึ่งอยู่ในระหว่างทดลองงาน ก็จะเลิกจ้างออกไป กรณีนี้จะต้องเติมข้อความใดลงไปในสัญญาจ้างบ้าง ? **218**
- (110) องค์กรเราสามารถเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกับองค์กรอื่นได้หรือไม่ ? **220**
- (111) บริษัททำสัญญาซื้อขายสินค้ากับผู้ค้ารายหนึ่ง โดยมีเงื่อนไขว่าทางผู้ค้าจะจัดส่งสินค้าที่ซื้อตามสัญญานั้นมาให้บริษัทของเรา แบบนี้ ผู้ซื้อหรือก็คือบริษัทของเราจะต้องให้ความยินยอมในการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้จัดส่ง (ซึ่งเป็นบุคคลที่สาม) หรือไม่ ? **221**
- (112) ส่ง Log ข้อมูลส่วนบุคคลของลูกค้าให้กับหน่วยงานภาครัฐที่มีอำนาจตามกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ.2562) แบบนี้ จะอ้างฐานการประมวลผลข้อมูลอะไรที่จะไม่ต้องขอความยินยอม ? **222**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (113) ตามปกติของการดำเนินธุรกิจ จะต้องมีการเปิดเผยข้อมูลให้แก่ผู้ขาย เช่น ในการสั่งซื้อสินค้าผ่านระบบออนไลน์ ผู้ซื้อจะต้องแจ้งชื่อที่อยู่และเบอร์โทรศัพท์ เพื่อการจัดส่งสินค้าไปยังบรรดาผู้ประกอบการที่ให้บริการขนส่งสินค้าผ่านทางเว็บไซต์ของผู้ซื้อ การเปิดเผยข้อมูลส่วนบุคคลไปยังผู้ประกอบการขนส่งนี้ ต้องอ้างอิงฐานใด ? **223**
- (114) อ่านในหนังสือ PDPA เล่ม 2 ของอาจารย์ (หน้า 152) เข้าใจว่ามาตรา 39 บางเรื่องยกเว้นสำหรับบริษัทขนาดเล็กไม่ต้องทำ ROPA แต่ที่ว่าขนาดเล็กนี้ แค่ไหนกัน ? **224**
- (115) ตามกฎหมาย การบันทึกรายการตามมาตรา 39 หรือ ทำ ROPA (จะเรียกว่า ROP ก็ได้) มี 8 เรื่องที่ต้องทำ แต่ดูแล้วจากที่อาจารย์แนะนำการจัดทำ DATA Discovery จะพบว่ามีส่วนซ้อนกันทีเดียวเลย ถ้าจัดทำแค่ Data Discovery แล้วใส่ว่า เป็น ROPA ได้หรือไม่ ? **225**
- (116) ถ้าลูกค้าขององค์กรทั้งหมด เป็นบริษัทหรือเป็นนิติบุคคล เราจำเป็นต้องทำ Privacy Notice สำหรับ **226**
- (117) การไปเอาข้อมูลของผู้สมัครงานมาจากเว็บที่ให้บริการรับสมัครงานเช่น JobsDB เราต้องส่ง Privacy Notice แจ้งเจ้าของข้อมูลให้ทราบด้วยหรือไม่ ? **227**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (118) สำหรับพนักงานที่ยังมีสถานะเป็นพนักงานของบริษัท อยู่ โดยตอนนี้ HR ยังไม่ได้ดำเนินการใด ๆ เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึง ขอคำแนะนำจากอาจารย์ว่าควรทำอะไรบ้าง ? **228**
- (119) องค์กรเก็บข้อมูลลายนิ้วมือหรือ Fingerprint ของพนักงานสำหรับเวลาผ่านเข้า-ออกที่ประตูด้านบริษัท หรือพื้นที่ควบคุมเป็นพิเศษใดใดเช่น ห้อง Server และก็ดึงเอาข้อมูลนี้ไปคำนวณเพื่อจ่ายค่าล่วงเวลา ค่าเบี้ยขยันและอื่นๆ ด้วย กรณีที่เราเริ่มเก็บข้อมูลนี้กันแล้ว เราต้องให้พนักงานในลงนามให้ความยินยอมหรือไม่ ? **229**
- (120) มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลต้องทำตามมาตรา 39 นั้น ต้องทำอะไรบ้างให้ครบถ้วนตามกฎหมาย ? **230**
- (121) บริษัทของเราทำเรื่องการขาย ต้องส่งต่อข้อมูลส่วนบุคคลที่เราขอความยินยอมจากลูกค้าแล้วไปให้กับบริษัทในเครือเพื่อทำเรื่องการตลาด แบบนี้ เราต้องระมัดระวังเรื่องใดบ้าง ? **232**
- (122) องค์กรจะกำหนดแนวทางหรือดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลอย่างไรดี ? **233**
- (123) ในแบบฟอร์มใบสมัครงาน ควรจะมีข้อความเรื่องใดบ้าง เพื่อให้เป็นไปตามกฎหมาย PDPA ? **235**
- (124) หากจะเขียนข้อความขอความยินยอมการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลสำหรับผู้สมัครงาน จะต้องเขียนประมาณใดดี ? **237**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (125) HR จำเป็นต้องเก็บข้อมูลส่วนบุคคลของบิดามารดา คู่สมรส และบุตรของพนักงานไว้เพื่อการบริหาร คำตอบแทน แบบนี้ ต้องขอความยินยอมจาก พนักงานและบุคคลเหล่านั้นหรือไม่ ? **241**
- (126) เปิดเผยข้อมูลเกี่ยวกับโรค Covid-19 ของพนักงาน จำเป็นที่จะต้องขอความยินยอมจากพนักงานรายหนึ่ง ใดนั้นหรือไม่ ? **242**
- (127) บริษัทว่าจ้าง Recruitment Agency เพื่อสรรหา พนักงาน โดยทางเราได้จัดทำ DPA ส่งไปให้ทาง บริษัท Recruitment Agency ดู แต่ทางนั้นบอกว่า เค้ามี NDA และก็เพียงพอกับการทำสัญญากันแบบนี้ เรายังต้องให้เราทำ DPA กับเค้าอีกหรือไม่ ? **245**
- (128) เราจ้างพนักงานของบริษัท Outsource มาทำงาน ให้กับเรา แบบนี้ เราต้องทำ DPA กับบริษัท Outsource / พนักงาน Outsource นี้หรือไม่ ? **247**
- (129) ลายมือชื่อ (ลายเซ็น) ของพนักงานเป็นข้อมูลส่วนบุคคลแบบอ่อนไหวหรือแบบทั่วไป ? **248**
- (130) แบบฟอร์มคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล จะใช้วิธีทำผ่านทางเว็บไซต์ หรือเป็นระบบ อิเล็กทรอนิกส์ได้หรือไม่ ? **249**
- (131) จะเขียน Privacy Notice สั้นและกระชับสำหรับลูกค้าที่ ต้องมาทำสัญญากับเราประมาณใดดี ? **251**
- (132) องค์กรควรเก็บรักษาข้อมูลส่วนบุคคลของผู้สมัคร งานไว้นานเพียงใด ? **253**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- (133) จะเขียนวัตถุประสงค์ ฐานการประมวลผลข้อมูล และ
การเปิดเผยข้อมูลส่วนบุคคลไว้ใน Privacy Notice
สำหรับกล่องวงจรปิด อย่างไรดี ? **254**
- (134) จะเขียนสิทธิของเจ้าของข้อมูลส่วนบุคคลในประกาศ
ความเป็นส่วนตัวหรือ Privacy Notice ไม่ว่าจะ
เรื่องใด อย่างไรดี ? **256**
- (135) จะแนะนำให้พนักงานประชาสัมพันธ์เพื่อให้การต้อนรับ
ผู้สมัครงานอย่างไรดี จึงจะไม่เสี่ยงกับการทำผิด
กฎหมาย PDPA ? **258**
- (136) บริษัทของเรา จะต้องจัดทำเอกสาร หรือขอความให้
ลูกค้าลงนามรับทราบหรือขอยินยอมหรือไม่ ? **260**
- (137) ควรประกาศให้พนักงานทราบว่า บริษัทกำลังทำตาม
กฎหมาย PDPA หรือกำลังจัดทำ PDPA Compli-
ance หรือไม่ ? **261**
- (138) พนักงานที่ทำงานเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะ
ของคู่ค้า ลูกค้า ผู้สมัครงาน หรือของพนักงาน แล้ว
นำเอาข้อมูลไปหาประโยชน์ (คือเอาข้อมูลไปขายให้คน
อื่น) มีความผิดตามกฎหมายหรือไม่ ? **262**
- (139) PDPA สำคัญกับ HR อย่างไร เราทำงานอยู่ตอนนี้
ไม่เห็นว่าการจัดการของ HR สนใจเรื่อง PDPA
อย่างที่เราสงสัยเลย ? **264**
- (140) มือใหม่ต้องทำเรื่องอะไรบ้างเพื่อให้เป็นไปตาม
กฎหมาย PDPA ? **268**

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

- | | |
|--|-----|
| (141) บันทึกรายการที่ผู้ควบคุมข้อมูลส่วนบุคคลต้อง ทำตามมาตรา 39 เรียกชื่อในภาษาอังกฤษว่า อย่างไรกันแน่ ? | 274 |
| (142) ทำไมจะต้องฝึกอบรมเรื่อง PDPA ให้กับพนักงานในองค์กรด้วย ? | 276 |
| (143) จะฝึกอบรมเรื่อง PDPA ให้กับพนักงานอย่างไรจึงจะได้ผลดี ? . | 279 |
| (144) บางองค์กรยักษ์ใหญ่ เคยทำสื่อประชาสัมพันธ์ให้ความรู้เรื่อง PDPA องค์กรขนาดเล็กไม่มีทรัพยากรอะไรขนาดนั้น แต่เราก็อยากให้ความรู้พนักงาน เราควรทำอย่างไรดี ? | 280 |
| (145) PDPA Awareness Training ต้องทำอะไร ? | 284 |
| (146) หากองค์กรของเราไม่ทำ PDPA จะมีปัญหาอะไรหรือไม่ ? | 288 |
| (147) โทษจากการไม่ปฏิบัติตามกฎหมาย PDPA มีอะไรบ้าง ขอคำแนะนำแบบแยกมาให้ชัดเลย ? | 290 |
| (148) พนักงานต้องระมัดระวังเรื่องใด เมื่อกฎหมาย PDPA บังคับใช้เต็มรูปแบบแล้ว ? | 297 |
| (149) ใช้เวลาสักเดือนนึง หรือประมาณต้นเดือนพฤษภาคม 2565 ค่อยทำ PDPA อาจารย์คิดว่าน่าจะเป็นวันที่ 1 มิถุนายน 2565 ที่กฎหมายจะบังคับใช้เต็มรูปแบบหรือไม่ ? | 300 |
| (150) ตอนนี้ มีเรื่องใดที่ต้องรอคณะกรรมการเข้าประกาศกำหนดรายละเอียดออกมาบ้าง ? | 306 |

สารบัญ (ต่อ)

150 คำถาม-คำตอบ PDPA

เนื้อหาสมนาคุณ (Bonus Content)

หลายเรื่องเข้าใจผิดเกี่ยวกับ PDPA ที่ “อย่าหากำ และอย่าได้จำ”	316
--	-----

ภาคผนวก

ก ประกาศกระทรวง DE ปี พ.ศ.2563	322
ข ประกาศกระทรวง DE (ฉบับที่ 2) ปี พ.ศ.2564	325
ค ตัวยกภาษาไทย กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act)	327

รู้จักผู้เขียน

ดร.ชัชวาล อรวงศ์สุภักดิ์	372
ยິงพร อินทร์ศรีชั้น	374

1

กฎหมาย PDPA คืออะไร ?

กฎหมาย PDPA หรือที่เราเรียกกันสั้น ๆ ว่า PDPA นั้น ก็คือกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือในภาษาอังกฤษก็จะเป็นคำว่า Personal Data Protection Act กฎหมายนี้ ตราขึ้นมาตั้งแต่ปี พ.ศ.2562 ที่ผ่านมา เพื่อกำหนดหลักเกณฑ์ กลไกและมาตรการในการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ในอันที่จะห้ามเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือไม่มีอำนาจที่กฎหมายบัญญัติเอาไว้ ทั้งนี้เพื่อเป็นหลักประกันการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

2

ประเทศอื่นเขามีกฎหมาย PDPA เหมือนประเทศไทยหรือไม่ ?

ในโลกใบนี้ การออกหรือการตรากฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไม่ใช่เรื่องใหม่ และก็ไม่ใช่ประเทศไทยเป็นประเทศเดียวที่มีกฎหมาย PDPA แม้จนถึงปัจจุบันที่ตีพิมพ์หนังสือเล่มนี้อยู่ (ตุลาคม 2564) ที่กฎหมาย PDPA ของบ้านเรายังไม่ได้ประกาศใช้เต็มรูปแบบ ในความเป็นจริงแล้ว มาเลเซียเองกลับเป็นประเทศแรกในกลุ่ม ASEAN ที่บังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล และก็น่าจะมีพัฒนาการของกฎหมายนี้ไกลกว่าบ้านเราอย่างมากเช่นกัน โดยมาเลเซียนั้นมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2010 (Malaysia Personal Data Protection Act 2010) กฎหมายนี้ ใช้บังคับกับบุคคลที่ไม่ได้อยู่ในประเทศมาเลเซีย แต่ใช้อุปกรณในประเทศมาเลเซียในการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากการส่งข้อมูลผ่านประเทศมาเลเซีย และใช้บังคับกับบุคคลที่ไม่ได้อยู่ในประเทศมาเลเซีย แต่ได้แต่งตั้งตัวแทนในประเทศมาเลเซียเพื่อวัตถุประสงค์ตามที่กฎหมายนี้ได้กำหนดไว้

ในประเทศสิงคโปร์ มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ค.ศ. 2012 (Personal Data Protection Act of 2012) เรียกว่ากฎหมาย PDPA ไม่แตกต่างจากบ้านเรา มีผลบังคับใช้อย่างสมบูรณ์เมื่อวันที่ 2 กรกฎาคม 2014 แตกต่างไปจากฟิลิปปินส์ ที่ได้ตรารัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 (Data Privacy Act of 2012) หรือ “DPA” เป็นต้น

ต้องบอกด้วยว่า ก่อนที่ประเทศต่าง ๆ จะออกกฎหมายนี้ออกมาเฉพาะ ก็มีหลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและกรอบข้อตกลงระหว่างประเทศ ได้แก่ (1) การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) (2) การคุ้มครองข้อมูลส่วนบุคคลตามข้อบังคับสหภาพยุโรป (European Union Directive 95/46/EC) และข้อตกลงรัฐสภายุโรป (3) กรอบการคุ้มครองข้อมูลส่วนบุคคลตามของสหประชาชาติ (United Nations) และ (4) กรอบการคุ้มครองข้อมูลส่วนบุคคลของ APEC เป็นต้น

ส่วนที่ยอมรับกันทั่วโลกนั้น น่าจะเป็น GDPR (General Data Protection Regulation) บังคับใช้กับประเทศในสหภาพยุโรป ซึ่งจะไม่ว่าในรายละเอียดนะ ตอนนี้พอรู้คร่าว ๆ ก่อนก็แล้วกัน

หากมองในเรื่องของการบังคับใช้กฎหมาย ต้องบอกว่ากฎหมาย PDPA ในประเทศไทยที่ออกมานี้ ก็มีลักษณะของการบังคับใช้ที่ไม่ได้แตกต่างไปจากกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่นแต่อย่างใดนะ โดยหลักแล้ว กฎหมายประเทศใด ก็จะบังคับใช้ได้ใรราชอาณาจักรของประเทศนั้น แต่คำว่าราชอาณาจักรนี้ ไม่ได้หมายถึงเฉพาะดินแดนไทยเท่านั้น เนื่องจากหลักดินแดนก็จะบอกว่า ราชอาณาจักรไทย เป็นต้น หมายความว่ารวมไปถึงอากาศยานไทย เรือไทย แล้วสถานกงสุลไทย ไม่ว่าจะอยู่ที่ประเทศใดก็ถือว่าเป็นราชอาณาจักรไทย (ประมวลกฎหมายอาญาว่าไว้แบบนั้น) ขอบเขตของการบังคับใช้กฎหมาย PDPA นี้ จึงครอบคลุมไปถึงผู้ประกอบการที่เป็นบุคคลธรรมดาหรือนิติบุคคลที่ตั้งในต่างประเทศ หากมีกิจกรรมการประมวลผลข้อมูล หรือพุดง่าย ๆ ก็คือมาเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของคน

ไทยแล้วล่ะก็ ต่อให้ตั้งบริษัทหรือสำนักงานของบริษัทอยู่ที่ต่างประเทศ ไม่ว่าจะทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรืออาจเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ก็ตาม ก็ไม่รอด.....ต้องทำตามกฎหมาย PDPA ของประเทศไทย ตัวอย่างเช่น บริษัทแห่งหนึ่งจดทะเบียนธุรกิจและตั้งอยู่ที่ต่างประเทศ แล้วทำการขายสินค้าผ่านระบบออนไลน์ให้กับคนไทย แต่ให้ทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลที่ต่างประเทศ ก็ต้องวากันตามกฎหมาย PDPA ของบ้านเรา

แต่เอ !!! มีเรื่องน่าคิดเหมือนกันนะว่า หากคนไทยซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลของตัวเองแล้ว เอาข้อมูลส่วนบุคคลของตนเองไปใช้ที่ต่างประเทศ แล้วจะต้องทำตามกฎหมายหรือเปล่านั้น ก็บอกก่อนว่า ตามกฎหมายก็ไม่ได้ครอบคลุมไปถึงการใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัว หรือเพื่อประโยชน์ในครอบครัว คือท่านจะเอาข้อมูลส่วนบุคคลของท่านไปใช้เอง ไม่ว่าจะใช้ในหรือต่างประเทศก็ตาม มันก็สิทธิในความเป็นส่วนตัวของท่าน เพียงแต่หากท่านเอาข้อมูลของท่านไปใช้ เช่น ซื้อของกับร้านค้าแห่งหนึ่งที่ต่างประเทศ ร้านค้าที่ต่างประเทศนั้น เจ้าก็ต้องทำตามกฎหมาย PDPA ของประเทศไทย แล้วอ้าว !!! ร้านค้าต่างประเทศ เจ้าจะรู้หรือว่า ท่านเป็นคนไทย แล้วกฎหมาย PDPA ของประเทศไทยเค้าว่าอย่างไร อันนี้ต้องบอกว่า ธรรมดาแล้ว การซื้อขายของ หากร้านค้าเค้าไม่ใช้ข้อมูลส่วนบุคคลแบบอ่อนไหวของท่าน เค้าก็สามารถอ้างฐานการปฏิบัติตามสัญญา (Contract) เพื่อที่จะไม่ต้องขอความยินยอมจากท่านได้อยู่แล้ว และหลักในเรื่องของการใช้ฐานการประมวลผลข้อมูลส่วนบุคคลของประเทศต่าง ๆ นั้น ก็มักจะไม่ได้แตกต่างกันมาก อย่างประเทศไทยนี้ ก็เป็นปรับเอาแนวของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของทางสหภาพยุโรปที่เรียกว่า GDPR มาปรับใช้เยอะมาก ซึ่ง GDPR ก็มีหลักการในเรื่องการใช้ฐานทางกฎหมายเพื่อการประมวลผลข้อมูลแทนการขอความยินยอม หรือการขอความยินยอมโดยชัดแจ้งอยู่แล้ว

จะว่าไปมันก็จะลำบากหน่อยตรงที่หากท่านไปทำธุรกรรมใดที่ต้องใช้ข้อมูลในประเทศใดที่เค้าไม่ได้มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ มันก็จะมีโอกาสที่ข้อมูลส่วนบุคคลของท่านจะรั่วไหลหรือไปใช้ประโยชน์ในทางที่มีขอบได้

และก็เป็นเหตุผลที่ว่า ในกฎหมาย PDPA ของบ้านเรานี้ ท่านก็จะได้เห็นบทบัญญัติในกฎหมายที่พูดถึงเรื่องการมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ “เพียงพอ” ซึ่งทางคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลท่านก็กำลังรวบรวมและคงจะประกาศให้เราทราบต่อไปในอนาคต (แต่ก็ไม่ต้องรู้อีกนานแค่นี้เหมือนกัน) ประเทศใดบ้างที่มีมาตรฐานการรักษาความมั่นคงปลอดภัยหรือมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ กว่าในประเทศ เช่นสหภาพยุโรป สหรัฐอเมริกา สหราชอาณาจักร สิงคโปร์ หรือแม้แต่บางประเทศเพื่อนบ้านของเรา เช่น ประเทศมาเลเซีย ก็ต้องบอกก่อนนะว่า เขาก็มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลมานานแล้ว เช่นที่ได้ยกตัวอย่างมาพูดถึงตอนต้นของเนื้อหาเรื่องนี้ไป

3

กฎหมาย PDPA สำคัญกับองค์กรอย่างไร ?

เวลาที่ไปอบรมเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้กับองค์กรทั้งหลาย สิ่งที่เราจะเริ่มต้นเล่าให้ฟังก่อนเลยก็คือ ความสำคัญของกฎหมายอันนี้ที่มีต่อองค์กร เนื่องจากธรรมดาแล้ว องค์กรจะทำเรื่องหนึ่งใดเร็วและแรงแค่ไหน (555) ก็มักจะขึ้นอยู่กับความสำคัญของมัน ซึ่งก็เป็นเรื่องปกติมาก เพราะงบประมาณมันก็มีจำกัด หรือแต่ให้มีเยอะก็ต้องใช้สอยอย่างประหยัด เป็นเพียงแต่ใครที่จะสะท้อนให้ผู้บริหารระดับสูงหรือเจ้าของธุรกิจโดยเฉพาะบรรดาเจ้าแก๊งทั้งหลาย เห็นความสำคัญเรื่องมันก็มีเท่านั้นละ

หากพิจารณาว่ากฎหมาย PDPA นี้สำคัญกับองค์กรอย่างไร โดยอยากบอกก่อนว่า ไม่ทำตามกฎหมายก็ผิดกฎหมาย จบนะ !!! แต่หากจะคุยกันอีกมุมหนึ่งก็ได้ ก็ขอหยิบมุมของประโยชน์ที่องค์กรจะได้รับจากการปฏิบัติหรือดำเนินการตามกฎหมายมาว่าก็แล้วกัน ซึ่งเรื่องนี้ ผู้รู้ท่านก็แนะนำไว้ในทำนองที่สอดคล้องกันเช่น การมีกฎหมายนี้ย่อมช่วยเพิ่มความเชื่อมั่นในมาตรฐานของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล หรือการจัดการข้อมูลต่อลูกค้า ลูกค้า หรือพันธมิตร ในการดำเนินงาน โดยเฉพาะเมื่อค้าขาย

กับองค์กรต่างประเทศที่อยู่ในประเทศของเขาบังคับใช้กฎหมายลักษณะนี้ด้วยแล้ว ก็ย่อมที่จะเป็นตัวช่วยสร้างความเชื่อมั่นในการค้าขายระหว่างกันในทางหนึ่ง และที่ว่าไปนี้ หากจะกล่าวว่าเป็นการเพิ่มขีดความสามารถในการแข่งขันขององค์กรก็ไม่ผิดนัก

มองในมุมหนึ่งได้ว่า หากองค์กรหรือบุคคลใดไม่ทำตามกฎหมาย PDPA จะเกิดอะไรขึ้น ตอบกันง่าย ๆ ตรงนี้เลยก็ผิดกฎหมาย PDPA นั่นเอง และตัวกฎหมายนี้ก็มีโทษสามแบบเลย ทั้งโทษอาญา (ปรับและจำคุก) โทษปรับทางปกครอง และโทษหรือความรับผิดชอบทางแพ่งจากการทำให้บุคคลอื่นได้รับความเสียหายทางละเมิด ที่สำคัญนั้นอย่าลืมดูมาตรา 81 ซึ่งสรุปความจากตัวบทกฎหมายได้ว่า หากผู้กระทำผิดกฎหมายนี้เป็นนิติบุคคล (ก็คือบริษัทหรือองค์กรภาครัฐที่ต้องปฏิบัติตามกฎหมายทั้งหลายนั้นละ) อันเป็นการกระทำผิดที่เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลนั้นมีหน้าที่ต้องสั่งการ หรือกระทำการ หรือละเว้นไม่สั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำผิด “ผู้นำ” ซึ่งก็หมายถึงกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ต้องรับโทษตามที่บัญญัติสำหรับความผิดนั้น ๆ ด้วย โดยเฉพาะหากความผิดตามกฎหมาย PDPA นั้นมีโทษจำคุก บุคคลที่เป็นกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล ก็อาจจะต้องรับโทษจำคุกด้วย

ถ้าแบบนี้ ก็ระมัดระวังกันเสียหน่อย จะเอาหูไปนา เอาตาไปไร่ ไม่ใส่ใจสนใจกฎหมาย PDPA แล้วหากเกิดปัญหาการละเมิดข้อมูลส่วนบุคคลของใครก็ตาม ไม่ว่าจะเป็นลูกค้า พนักงาน ผู้สมัครงาน ก็อาจจะเคลียร์ไม่ไหว ตั้งรับไม่ทันสถานการณ์ก็ได้ เราแนะนำว่าอย่าประมาทไป เดี่ยวจะเข้าทำนองเสียน้อยเสียยาก เสียมากเสียง่าย และบานปลายไปถึงเรื่องการเสื่อมเสียภาพลักษณ์ขององค์กร ซึ่งก็ต้องยอมรับกันว่า กว่าจะสร้างภาพลักษณ์องค์กรให้ดีงามได้มาจนถึงวันนี้ มันไม่ง่ายและใช้งบประมาณไปก็น่าจะไม่น้อย แต่อาจจะต้องมาเสียไปแบบง่าย ๆ เพียงเพราะอารมณ์ประมาณว่า เสียเวลา

ยังกับผู้บริหารมืออาชีพที่องค์กรเค้าว่าจ้างมาทำงาน ย่อมเป็นที่คาดหวังว่าจะต้องไม่ทำผิดกฎหมายเสียเอง แต่ด้วยความบางท่านก็คิดแต่ว่าเสียเวลาทำมาหารายได้ ทำตามกฎหมาย PDPA

มีแต่เสียเงิน หากเกิดเรื่องราวละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมา ก็อาจจะถูกเล่นงานหนักจากผู้ถือหุ้นที่เป็นเจ้าขององค์กรตัวจริงเอาได้ น่าเสียดายความเป็นนักบริหารมืออาชีพแต่ต้องมาตกม้าตายกับเรื่องที่ไม่ทำตามกฎหมาย PDPA นี้

ผู้ประกอบการหลายท่านไม่ได้สนใจกฎหมาย PDPA เพราะเคยมีประสบการณ์กับกฎหมายความปลอดภัยมาแล้วพบว่าไม่มีใครมาตรวจสอบว่าองค์กรได้ทำเรื่องความปลอดภัย อาชีวอนามัยและสภาพแวดล้อมในการทำงานหรือไม่ เพียงใดก็เลยชะล่าใจ เพราะล้าพังพนักงานไม่มีใครไปร้องเรียนอยู่แล้ว แต่กับกฎหมาย PDPA เจ้าของข้อมูลส่วนบุคคลนั้นไม่ได้มีแต่พนักงานอย่างเดียว ยังมีลูกค้า คู่ค้า และผู้สมัครงานอีกด้วย เราจะทำงานแบบ “วัดใจ” กับบุคคลเหล่านี้หรือไม่ว่าเขาจะไม่ไปร้องเรียนการกระทำผิดกฎหมาย PDPA ขององค์กรของเรา

เรื่องนี้ เดี่ยวไปว่ากันยาว ๆ ในบางหัวข้อคำถามตอนท้ายเล่มอีกครั้งนึง

ขยายความหน่อยว่า การจัดทำงานต่าง ๆ ขององค์กรให้สอดคล้องกับกฎหมาย PDPA หรือเรียกกันแบบเข้าใจง่าย ๆ ว่า Implement กฎหมาย PDPA ในองค์กรนั้น นอกเหนือจากลดความเสี่ยงในการที่จะต้องรับผิดตามกฎหมายทั้งจากความจงใจ ความประมาทเลินเล่อ หรือจากการโจรกรรมข้อมูลของบรรดามิจฉาชีพที่ไม่หวังดีแล้ว ก็ต้องยอมรับว่าเป็นเรื่องที่จะช่วยเสริมสร้างภาพลักษณ์ที่ดีให้แก่องค์กร ยิ่งในยุคนี้ ยุคที่คนทำงานหนุ่มสาวรุ่นใหม่ ไม่ได้มองหาองค์กรร่วมงานที่ใหญ่โตมั่งคั่งเท่านั้น หากแต่ยังต้องการทำงานกับองค์กรที่มีภาพลักษณ์ที่ดี ตอบแทนสังคม ทำตามกฎหมาย ไม่เห็นแก่รักรวยโดยไม่แยแสสนใจการปฏิบัติตามกฎหมาย โดยเฉพาะเฮียรวยแต่เอาเปรียบลูกน้องแบบนี้ องค์กรหากคนทำงานรุ่นใหม่ยากเป็นแน่ และการทำตามกฎหมาย PDPA ก็เป็นสิ่งที่องค์กรสามารถนำเอาไปป่าวประกาศให้สังคมได้รู้เลยว่า องค์กรใส่ใจกับการเป็น “พลเมืององค์กร” ที่ดีของสังคม

ยิ่งกับองค์กรที่มีสำนักงานใหญ่หรือบริษัทแม่ที่ต่างประเทศ ก็หรือองค์กรที่เป็นบริษัทมหาชนจำกัด ยิ่งต้องซีเรียสกับเรื่องการทำ

ตามกฎหมาย แม้จะต้องลงทุนลงแรง ใช้งบประมาณเพื่อการทำให้เกิดขึ้นในองค์กรก็ต้องเจียดจ่ายเงินและกำลังคนมาทำ เพราะมันสำคัญ ถึงขนาดที่ประเทศไทยของเรา ออกเป็นกฎหมายออกมาเลยทีเดียว

นอกเหนือจากนี้ ปฏิเสธไม่ได้เลยว่าการ Implement กฎหมาย PDPA ในองค์กรของเรา ย่อมเป็นปัจจัยเงื่อนไขหนึ่งที่ทำให้เกิดให้องค์กรเกิดความได้เปรียบในการแข่งขัน โดยเฉพาะเมื่อเทียบกับองค์กรคู่แข่งที่ไม่ได้ทำให้สอดคล้องกับกฎหมาย PDPA เหมือนอย่างองค์กรของท่าน ลองคิดตามดูว่า หากองค์กรของท่านทำ PDPA ในขณะที่องค์กรคู่แข่งไม่ได้ทำ และทั้งเราและคู่แข่งต่างก็ขายสินค้าหรือให้บริการไม่ได้แตกต่างกันมากนัก ท่านคิดว่าองค์กรลูกค้าของเรา อาจจะเลือกใช้บริการจากท่านหรือของคู่แข่งล่ะ

ท่านจึงควรที่จะต้องทำ PDPA และบอกกับลูกค้าหรือว่าที่ลูกค้าของท่านนั้นท่านใส่ใจกับการปฏิบัติตามกฎหมาย PDPA นี้ไหม ๆ ก็ลงทุนลงแรงแล้ว ก็ป่าวประกาศให้สังคมรู้เสียหน่อยไปเลยก็ไม่เลว นัยว่า “เกทับ” คู่แข่งเสียหน่อยก็คงเป็นการดีไม่น้อย

อีกเรื่องหนึ่งการทำ PDPA ก็ดีไม่น้อย เพราะมันสอดคล้องกับข้อกำหนดของมาตรฐานคุณภาพระดับโลกเช่น ISO 27001 หรือเรื่องอื่น ๆ ที่น่าจะมีติดตามมาอีกมากมาย มันก็ช่วยเสริมสร้างทั้งภาพลักษณ์และสร้างความแข็งแกร่งให้กับระบบงานอีกทางหนึ่ง

4

ข้อมูลส่วนบุคคล (Personal Data) คืออะไร ?

ตามความในมาตรา 6 ของกฎหมาย PDPA “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ข้อมูลส่วนบุคคลตามกฎหมายนี้ จึงเป็นข้อมูลของบุคคลธรรมดาเท่านั้น ข้อมูลนิติบุคคล ข้อมูลคนที่เสียชีวิตไปแล้ว หรือข้อมูลคนตาย และข้อมูลที่นิรนาม (Anonymous Data) ที่ไม่สามารถระบุตัวตนของบุคคลธรรมดาได้ จึงไม่ได้เป็นข้อมูลที่ต้องว่ากันตามกฎหมายนี้แต่อย่างใด

ขยายความได้ว่า ข้อมูลส่วนบุคคลหรือ Personal Data นี้ เป็นข้อมูล สารสนเทศ เรื่องราวหรือข้อเท็จจริง อันทำให้สามารถระบุตัวตนของบุคคลธรรมดาคนหนึ่งได้ ไม่ว่าจะระบุทางตรงหรือระบุทางอ้อมก็ตาม และบุคคลนั้น ต้องไม่ใช่นิติบุคคล (บุคคลสมมติตามกฎหมาย) การกระทำต่อข้อมูลของนิติบุคคล ไม่ว่าจะอยู่ในรูปขององค์กรธุรกิจเช่น บริษัท ห้างร้านต่าง ๆ รวมทั้งองค์กรที่อาจจะไม่แสวงหากำไร อันได้แก่ มูลนิธิ สมาคมทั้งหลาย ตลอดจนจนถึงหน่วยงานของภาครัฐ (Public Authority) ก็ไม่เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมายนี้

และที่สำคัญ บุคคลที่จะเป็นเจ้าของข้อมูลส่วนบุคคลได้นั้น จะต้องเป็น “สภาพเป็นบุคคลด้วย” หากตายไปแล้ว ก็ย่อมสิ้นสภาพของบุคคลไปตามที่กฎหมายกำหนดไว้ หรือกล่าวอย่างง่าย ๆ ก็คือ บุคคล นอกเหนือจากจะไม่เป็นนิติบุคคลแล้ว จะต้องไม่ใช่คนตายที่หมดสภาพความเป็นบุคคลตามกฎหมายไปแล้วนั่นเอง

แต่หากข้อมูลของบริษัท ห้างร้านข้อมูลใด แม้จะไม่ใช่ข้อมูลบุคคลธรรมดา แต่หากมันเป็นข้อมูลที่สามารถสืบสาวย้อนกลับไปถึงระบุตัวบุคคลธรรมดา เช่น เป็นข้อมูลที่บ่งชี้มาถึงนายชัชวาล อรรถศรีสุภักดิ์ หรือนางสาวยิ่งพร อินทร์ศรีชื่น ได้ แบบนี้ ข้อมูลที่ว่าจะเป็น “ข้อมูลส่วนบุคคล” เช่นกัน

ซึ่งท่านทั้งหลายก็จะเห็นว่ามันจะมีเยอะรายการมากนั่นเอง

อย่างไรก็ตาม มีเอกสารสำคัญของนิติบุคคลจำพวกที่ระบุตัวของการกรรมการผู้มีอำนาจลงนามผูกพัน หรือกรรมการอื่น ซึ่งสามารถระบุตัวตนของบุคคลธรรมดาได้ ผู้เชี่ยวชาญท่านระบุไว้ว่า ข้อมูลเหล่านี้ ไม่ได้เป็นข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมาย PDPA แต่อย่างใด ในต่างประเทศที่ใช้กฎหมาย GDPR ก็มีแนวปฏิบัติที่ยึดถือเช่นนี้ กระนั้น ก็ไม่อาจสรุปได้ในทุกกรณีว่า ข้อมูลของการกรรมการผู้มีอำนาจนั้น จะไม่ใช่ข้อมูลส่วนบุคคลตามกฎหมาย PDPA เพราะหากเป็นข้อมูลของบุคคลที่ประกอบกิจการในรูปบุคคลธรรมดา แล้วไปทำนิติกรรมหรือสัญญาใดใดโดยไม่จดทะเบียนนิติบุคคลแล้ว ข้อมูลของผู้ประกอบการคนเดียวที่ว่่านั้น ก็เป็นข้อมูลส่วนบุคคล

5

ข้อมูลส่วนบุคคลมีกี่แบบ ?

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 ใช้หรือเปิดเผย หรือเรียกว่า “การประมวลผลข้อมูล” พุดง่าย ๆ ได้ว่ากฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลแบบทั่วไปนั่นเอง

(1) ข้อมูลส่วนบุคคลแบบทั่วไป

พูดอย่างรวบรัดได้ว่า ข้อมูลส่วนบุคคลแบบทั่วไปนั้นก็คือข้อมูลส่วนบุคคลแบบที่ไม่ได้เป็นข้อมูลอ่อนไหวตามมาตรา 26 นั่นเอง โดยเป็นข้อมูลส่วนบุคคลที่มีหลักทั่วไปในการจัดเก็บรวบรวมตามที่มาตรา 24 กำหนด เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์มือถือ เป็นต้น

(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

ตอนนี้ (ณ เวลาที่เขียนหนังสือนี้) ข้อมูลอ่อนไหว (Sensitive Data) มี 12 อย่าง

- 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 ซึ่งอาจจะเป็นประวัติการลงโทษทางวินัยของพนักงาน ข้อมูลค่าจ้าง เงินเดือน ค่าตอบแทนของพนักงาน ก็เป็นได้ ก็ต้องรอฟังจากประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต่อไป

คราวนี้อยากให้ท่านมาเรียนรู้หน่อยว่า ข้อมูลส่วนบุคคลบางอย่างต่อไปนี้ ตกลงแล้ว มันเป็นข้อมูลอ่อนไหว (Sensitive Data) หรือไม่ และหากมันเป็นข้อมูลอ่อนไหวแล้ว มันคือข้อมูลใดกันแน่ เพื่อที่จะได้ไปกำหนดฐานการประมวลผลข้อมูลและทำเรื่องอื่น ๆ ที่เกี่ยวข้องได้ตรงจุดมากขึ้น โดยเราได้รวบรวมจากบรรดาคำถามที่ผู้เข้ารับการอบรม และบุคลากรของหลายองค์กรที่เราเป็นที่ปรึกษาทำการ Implement PDPA มาแจกแจงตอบให้

ลองตอบคำถามในตารางนี้:

รายการข้อมูลส่วนบุคคล	เป็น	ไม่เป็น	คำอธิบาย
ข้อมูลหมู่โลหิตหรือ Blood Group			
ข้อมูลผลการปฏิบัติงานหรือเกรดของพนักงาน (Performance Grade)			
ข้อมูลการลงโทษทางวินัยพนักงาน			
ใบนัดพบพบแพทย์ (ใบนัดหมอ)			
ลายนิ้วมือของพนักงานที่ประทับบนเอกสาร (ไม่ใช่ที่ใช้ตอนสแกนผ่านเข้าออกที่ประตู)			
ข้อมูลเงินเดือนค่าจ้าง และสิทธิประโยชน์ของพนักงาน			
ข้อมูลสัญชาติ (Nationality) ของพนักงาน			

เป็นอีกครั้งนะ ข้อมูลส่วนบุคคลตามตารางข้างต้นนี้ เป็นข้อมูลอ่อนไหว (Sensitive Data) หรือไม่ ???

หากจะตอบแบบซัวร์ ๆ คงต้องไม่ลืม “ย้อนกลับ” ไปดูที่หน้า 10 หากดูแล้วมันมีใน 11 รายการ (รายการที่ 12 ทางคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลท่านจะได้กำหนดต่อไปในภายหลัง) หากพบว่ามันมีอยู่ใน 11 รายการนั้น มันก็เป็นข้อมูลอ่อนไหว แต่หากมันไม่อยู่ใน 11 รายการ มันก็ไม่ใช่ ก็เป็นเพียงข้อมูลทั่วไปเท่านั้น

จากที่ตามไป ก็จะได้คำตอบและคำอธิบายประมาณนี้....

รายการข้อมูลส่วนบุคคล	เป็น	ไม่เป็น	คำอธิบาย
ข้อมูลหมู่โลหิต (Blood Group)	✓		เป็นข้อมูลพันธุกรรม
ข้อมูลผลการปฏิบัติงาน		✓	อาจจะอ่อนไหวในความรู้สึกเท่านั้น
ข้อมูลการลงโทษทางวินัย พนักงาน		✓	เพราะไม่ใช่ประวัติ อาชญากรรมทาง อาญาแต่อย่างใด
ใบนัดพบพบแพทย์ (ใบนัดหมอ)	✓	✓	ใบนัดพบแพทย์ที่มี ข้อมูลสุขภาพ จะเป็น ข้อมูลอ่อนไหว แต่ถ้ามี เพียงกำหนดวันเวลา นัดพบแพทย์เท่านั้น เป็นเพียงข้อมูลทั่วไป
ลายนิ้วมือของพนักงาน (Employee Fingerprint)	✓	✓	ลายนิ้วมือของ พนักงานที่ประทับบน เอกสารเป็นข้อมูล ทั่วไป แต่หากเป็น ลายนิ้วมือจำลองที่ใช้ ตอนสแกนผ่านเข้า ออกที่ประตูที่ทำงาน จะเป็นข้อมูลอ่อนไหว (เป็นข้อมูลชีวภาพ)
ข้อมูลเงินเดือนค่าจ้าง และสิทธิ ประโยชน์ของพนักงาน		✓	อาจจะอ่อนไหวใน ความรู้สึกเท่านั้น
ข้อมูลสัญชาติ (Nationality) ของพนักงาน		✓	ข้อมูลเชื้อชาติจึงจะ เป็นข้อมูลอ่อนไหว

6

ข้อมูลส่วนบุคคล (Personal Data) ของลูกค้าและ คู่ค้ามีอะไรบ้าง ?

การหาให้พบว่ามีข้อมูลส่วนบุคคล (Personal Data) ของลูกค้าหรือคู่ค้าที่ใดบ้าง เก็บไว้ที่ใดบ้างในฐานข้อมูล หรือไฟล์ หรือระบบอะไรต่าง ๆ มีประโยชน์อย่างมากกับการเอามาวิเคราะห์เพื่อกำหนดฐานการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) แต่บางทีก็นึกไม่ออกว่าข้อมูลส่วนบุคคลของลูกค้าหรือคู่ค้านั้นมีอะไรบ้าง

- ข้อมูลสำเนาเอกสารที่สามารถใช้เพื่อระบุตัวตนของลูกค้าหรือคู่ค้า ซึ่งเราต้องนำมาประกอบการให้บริการ หรือการทำงานร่วมกัน เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง เอกสารอื่น ๆ ที่ออกให้โดยหน่วยงานของรัฐ ทะเบียนราษฎร
- ข้อมูลในการติดต่อของลูกค้าหรือคู่ค้า เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อีเมล ข้อมูลโซเชียลมีเดีย (เฉพาะที่เป็นบุคคลธรรมดา)
- ข้อมูลเกี่ยวกับตัวของลูกค้าหรือคู่ค้า เช่น วันเดือนปีเกิด อายุ เพศ สถานะการสมรส ความสนใจ ความคิดเห็นทางการเมือง
- ข้อมูลเกี่ยวกับสมาชิกครอบครัวหรือผู้อยู่ในความดูแลของลูกค้าหรือคู่ค้าที่มีสิทธิได้รับประโยชน์จากสินค้าหรือบริการ เช่น ข้อมูลเกี่ยวกับคู่สมรส ข้อมูลเกี่ยวกับข้อมูลเกี่ยวกับบิดามารดา ผู้รับผลประโยชน์ เป็นต้น
- ข้อมูลเกี่ยวกับการศึกษา ความสามารถ และคุณสมบัติอื่น ๆ ของลูกค้าหรือคู่ค้า เช่น ระดับการศึกษา วุฒิการศึกษา สถาบัน/มหาวิทยาลัย ประวัติการศึกษา ประวัติการฝึกผลการศึกษา ผลการทดสอบ ความสามารถอื่น ๆ ที่เราต้องใช้เพื่อการให้บริการหรือทำงานด้วย
- ข้อมูลเกี่ยวกับประสบการณ์ทำงาน หรือประสบการณ์การให้บริการของลูกค้าหรือคู่ค้าแล้วแต่จะจัดเก็บ

บางทีเราอาจจะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือคู่ค้าอีกส่วนหนึ่งที่เป็นข้อมูลอ่อนไหวหรือ Sensitive Data ได้แก่

- ข้อมูลส่วนบุคคล (Personal Data) ของลูกค้าและข้อมูลสุขภาพ เช่น น้ำหนัก ส่วนสูง โรคประจำตัว โรคตาบอดสี ผลการตรวจร่างกาย ข้อมูลการแพ้อาหาร ข้อมูลการแพ้ยา หมู่โลหิต ใบรับรองแพทย์ ประวัติการรักษายาบาล ประวัติการรักษายาบาล
- ข้อมูลชีวภาพ (Biometric Data) เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองลายนิ้วมือ ข้อมูลจำลองม่านตา ข้อมูลอัตลักษณ์เสียง เพื่อวัตถุประสงค์ในการพิสูจน์และยืนยันตัวตนของลูกค้าบริการที่ขอสมัคร และ/หรือทำธุรกรรมผ่านช่องทางต่าง ๆ ที่องค์กรให้บริการ หรือของคู่ค้าที่จะต้องใช้ประสานงานกับองค์กร

ที่ว่ามานี้คงเป็นเพียงส่วนหนึ่งเท่านั้น ข้อมูลส่วนบุคคลของลูกค้าและคู่ค้า จะมีเยอะมาก ซึ่งไม่ว่าจะมาก หรือไม่มาก เพียงใดก็ตาม ก็ต้องหาให้พบทั้งหมด ซึ่งหลายองค์กรก็จะใช้ Software การค้นหาและวิเคราะห์ข้อมูลเช่น Data Discovery Software มาช่วยซึ่งก็ควรต้องเป็นแบบนั้นล่ะ

7

ข้อมูลส่วนบุคคลของพนักงาน (Employee Personal Data) มีอะไรบ้าง ?

ลองมา List ดูว่า ข้อมูลส่วนบุคคลของพนักงานในองค์กรขององค์กรมีอะไรบ้าง โดยก่อนอื่น อยากรแนะนำให้ไปทบทวนความหมายและประเภทของข้อมูลส่วนบุคคล (Personal Data) ในตอนก่อนหน้าก่อน และแน่นอนว่าองค์กรสามารถนำเอาข้อมูลเหล่านี้ไปเขียนไว้ในนโยบายความเป็นส่วนตัวสำหรับพนักงาน (Privacy Policy for Employee) ขององค์กรได้ และแนะนำให้ลองนำไปปรับใช้กับองค์กรของท่านดู

- ข้อมูลสำเนาเอกสารที่สามารถใช้เพื่อระบุตัวตนของพนักงาน เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง เอกสารอื่น ๆ ที่ออกให้โดยหน่วยงานของรัฐ ทะเบียนราษฎร

- ข้อมูลเกี่ยวกับตัวของพนักงาน เช่น วันเดือนปีเกิด อายุ เพศ สถานะการสมรส ความสนใจ ความคิดเห็น
- ข้อมูลและเอกสารที่เกี่ยวข้องกับกระบวนการสรรหาพนักงาน เช่น ประวัติส่วนบุคคล (Resume/CV) จดหมายสมัครงาน ใบสมัครงาน รวมทั้งความเห็นประกอบการสรรหาพนักงาน
- ข้อมูลเกี่ยวกับสมาชิกครอบครัวหรือผู้อยู่ในความดูแลของพนักงานที่มีสิทธิได้รับสวัสดิการตามข้อบังคับและระเบียบการบริหารงานบุคคลของบริษัท เช่น ข้อมูลเกี่ยวกับคู่สมรส ข้อมูลเกี่ยวกับบิดามารดา ผู้รับผลประโยชน์ ทั้งนี้ ก่อนการให้ข้อมูลกับองค์กร ให้พนักงานแจ้งนโยบายความเป็นส่วนตัวส่วนตัวนี้ ให้บุคคลดังกล่าวทราบด้วย
- ข้อมูลรูปถ่ายและภาพเคลื่อนไหว
- ข้อมูลเกี่ยวกับการศึกษา ความสามารถ และการพัฒนา ศักยภาพ และคุณสมบัติอื่น ๆ ของพนักงาน เช่น ระดับการศึกษา วุฒิการศึกษา สถาบัน/มหาวิทยาลัย ประวัติการศึกษา ประวัติการฝึกผลการศึกษา ผลการทดสอบ สิทธิในการทำงานอย่างถูกต้องตามกฎหมาย คุณสมบัติด้านวิชาชีพ ความสามารถทางด้านภาษา และความสามารถอื่น ๆ
- ข้อมูลเกี่ยวกับประสบการณ์ทำงานและข้อมูลเกี่ยวกับการจ้างงานในอดีต เช่น ตำแหน่งงาน รายละเอียดของนายจ้าง เงินเดือนและค่าตอบแทน สวัสดิการที่ได้รับ
- ข้อมูลเกี่ยวกับสถานที่ที่สามารถปฏิบัติงานได้
- ข้อมูลข้อมูลเกี่ยวกับภาระทางทหาร (Military Service) เช่น การผ่านการเกณฑ์ทหาร การเข้ารับการฝึกทางทหาร ในภาคสนาม ข้อมูลการเรียกระดมพลอื่น ๆ เป็นต้น
- ข้อมูลเกี่ยวกับลักษณะของพนักงาน เช่น นิสัย พฤติกรรมทัศนคติ ความถนัด ทักษะ ภาวะความเป็นผู้นำ ความสามารถในการทำงานร่วมกับผู้อื่น ความฉลาดทางอารมณ์ ความผูกพันต่อองค์กร อันอาจได้มาจากการสังเกตและวิเคราะห์ขององค์กรและพนักงานขององค์กรในระหว่างการปฏิบัติงานหรือเข้าร่วมกิจกรรมกับองค์กร

- ข้อมูลที่จำเป็นสำหรับการรายงานหน่วยงานที่ทำกับดูแล เช่น กระทรวงแรงงาน ตลาดหลักทรัพย์แห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- ข้อมูลทางการเงิน เช่น ข้อมูลค่าจ้าง เงินเดือน รายได้ ภาษี กองทุนสำรองเลี้ยงชีพ บัญชีการกู้ยืมเงิน รายการยกเว้น หรือหักลดหย่อนทางภาษี การถือหลักทรัพย์ของบริษัทในบริษัทหลักทรัพย์
- ข้อมูลที่เกี่ยวข้องกับการประกันสังคม การคุ้มครองแรงงาน สิทธิประโยชน์ สวัสดิการ และผลประโยชน์ที่พนักงานได้รับ หรือมีสิทธิที่จะได้รับตามข้อบังคับและระเบียบเกี่ยวกับการบริหารงานบุคคลขององค์กร
- ข้อมูลบันทึกการเข้าออกงานและระยะเวลาในการปฏิบัติงาน การทำงานล่วงเวลา การขาดและลางาน
- ข้อมูลประวัติการปฏิบัติงาน ตำแหน่งงาน การเข้าประชุม การให้ความเห็นในการที่เป็นกรรมการบริษัท จะมีการเพิ่มเติมข้อมูล ประวัติกรรมการ ทะเบียนกรรมการด้วย
- ข้อมูลการใช้งานและการเข้าถึงระบบสารสนเทศ คอมพิวเตอร์ ระบบงาน เว็บไซต์ แอปพลิเคชัน ระบบโครงข่าย อุปกรณ์อิเล็กทรอนิกส์ ระบบอีเมล เพื่อให้สอดคล้องกับนโยบายเทคโนโลยีสารสนเทศขององค์กร และกฎหมายที่เกี่ยวข้อง
- ข้อมูลที่รวบรวมจากการมีส่วนร่วมขององค์กร เช่น การเข้าร่วมกิจกรรม การตอบแบบสำรวจ การตอบแบบประเมิน
- ข้อมูลอื่นที่จำเป็นต่อการตรวจสอบความขัดแย้งทางผลประโยชน์ เช่น ข้อมูลข้อมูลการถือหุ้นและความสัมพันธ์กับคู่ธุรกิจ
- ข้อมูลเกี่ยวกับอุบัติเหตุ ทั้งในกรณีที่พนักงานประสบอุบัติเหตุในเวลางานหรืออันเนื่องมาจากการปฏิบัติงาน และอุบัติเหตุอื่น ๆ

นี่เป็นตัวอย่างของข้อมูลส่วนบุคคลของพนักงานเท่านั้น อันที่จริงยังมีข้อมูลอีกหลายรายการเลย และก็ยังต้องมีข้อมูลส่วนบุคคลของพนักงานอีกส่วนหนึ่งที่เป็นข้อมูลส่วนบุคคลแบบอ่อนไหวหรือ Sensitive Data ซึ่งได้แก่