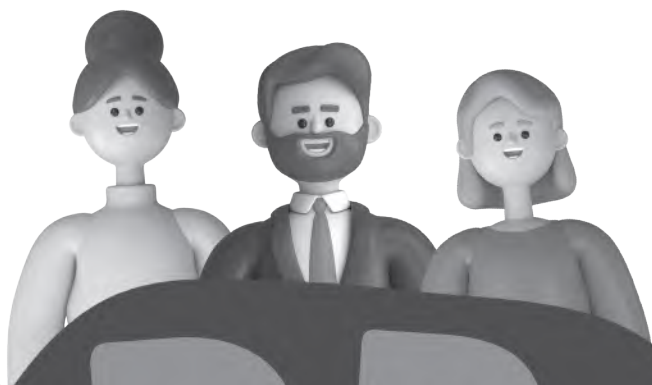




P D P A *for* H R

จากกฎหมายสู่การปฏิบัติ
เข้าใจง่าย ใช้ได้จริง

รับขวัญ ชลดำรงศกุล



PDPA *for* HR

จากกฎหมายสู่การปฏิบัติ
เข้าใจง่าย ใช้ได้จริง

PDPA *for* HR

จากกฎหมายสู่การปฏิบัติ เข้าใจง่าย ใช้ได้จริง

โดย รัชวัณ ชลดำรงกุล

พิมพ์ครั้งแรก : พฤศจิกายน 2568

เจ้าของ : บริษัท ธรรมนิติ เพรส จำกัด
ที่ปรึกษา : ดารารัตต์ พิชมงคล
กองบรรณาธิการ : ศศิพันธุ์ อุษณีย์มาศ
พิสูจน์อักษร : ประนอม เพ็ชรสมัย / จันทรีจิรา ชื้อพร้อม
จัดรูปเล่ม : จีรนนท์ ทับสุข
ประสานงาน : ทิพสุคนธ์ วงษ์เมือง

ได้รับอนุญาตจัดพิมพ์จากเจ้าของลิขสิทธิ์ถูกต้องตามกฎหมาย สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537
(ห้ามลอกเลียนแบบไม่ว่าส่วนหนึ่งส่วนใดของหนังสือเล่มนี้ รวมทั้งการจัดเก็บ ถ่ายทอด ไม่ว่ารูปแบบหรือวิธีการใดๆ

ด้วยกระบวนการทางอิเล็กทรอนิกส์ การถ่ายภาพ การบันทึก หรือวิธีการอื่นใดโดยไม่ได้รับอนุญาต

มิฉะนั้นจะถือว่ามีความผิดตามกฎหมาย)

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

รัชวัณ ชลดำรงกุล.

PDPA for HR จากกฎหมายสู่การปฏิบัติ เข้าใจง่าย ใช้ได้จริง.

-- กรุงเทพฯ : ธรรมนิติ เพรส, 2568.

496 หน้า.

1. การป้องกันข้อมูล -- กฎหมายและระเบียบข้อบังคับ. I. ชื่อเรื่อง.

342.0585

ISBN : 978-616-302-529-6

จัดพิมพ์และจำหน่ายโดย

บริษัท ธรรมนิติ เพรส จำกัด

178 อาคารธรรมนิติ ชั้น 4 ซอยเพิ่มทรัพย์ (ประตูซิ่น 20)

ถนนประตูซิ่น แขวงบางซื่อ เขตบางซื่อ กรุงเทพฯ 10800

โทรศัพท์ (02) 555-0713 โทรสาร (02) 555-0728

สนใจเสนอผลงานเขียนเพื่อตีพิมพ์กับธรรมนิติ ได้ที่ E-mail : book@dharmainiti.co.th

คำนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่เรียกกันคุ้นหูว่า PDPA นับเป็นกฎหมายที่ทุกองค์กรต้องให้ความสำคัญ โดยเฉพาะฝ่ายทรัพยากรบุคคลหรือฝ่าย HR ซึ่งเกี่ยวข้องโดยตรงกับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของพนักงานที่เป็น “บุคคลธรรมดา” (ซึ่งถือเป็นกลุ่มเจ้าของข้อมูลส่วนบุคคลตามนิยามกฎหมายอย่างชัดเจน) ในทุกขั้นตอน ตั้งแต่การรับสมัคร การบริหารงาน ไปจนถึงการสิ้นสุดการจ้าง ดังนั้นเมื่อบริษัทเริ่มมีพนักงานคนแรก บริษัทไม่ว่าเล็กหรือใหญ่ก็มีหน้าที่ต้องทำความเข้าใจและปฏิบัติตามกฎหมาย PDPA ทันที

และเมื่อเป็นเรื่องกฎหมาย หลาย ๆ คน จึงรู้สึกว่าเป็นเรื่องยาก แต่ถ้าบริษัทเข้าใจหลักการของ PDPA แล้ว การปฏิบัติตามเพื่อรับประกันความสอดคล้องถูกต้องตามกฎหมาย และการเพิ่มความเชื่อมั่นให้แก่บุคลากรขององค์กรย่อมไม่ใช่เรื่องยาก

หนังสือ PDPA for HR จากกฎหมายสู่การปฏิบัติ เข้าใจง่ายใช้ได้จริง ผู้เขียนตั้งใจจัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติอย่างเป็นระบบแบบเข้าใจง่าย ช่วยให้ฝ่าย HR และผู้เกี่ยวข้องเข้าใจหลักการสำคัญของกฎหมาย พร้อมแนวทางและแบบฟอร์มนำไปใช้ในสถานการณ์จริง เช่น การจัดทำประกาศความเป็นส่วนตัว (Privacy Notice) การขอความยินยอม การกำหนดระยะเวลาเก็บรักษาข้อมูลรวมถึงแนวทางการจัดการเมื่อเกิดเหตุข้อมูลรั่วไหล เนื้อหาครอบคลุมทุกช่วงของวงจรการทำงาน ตั้งแต่การบริหารข้อมูลของผู้สมัครงาน พนักงานปัจจุบัน พนักงานที่ลาออก ตลอดจนผู้ให้บริการภายนอก เพื่อให้นำไปปรับใช้ได้จริงในองค์กร

เพราะการเข้าใจ PDPA ไม่ใช่แค่ทำให้ถูกกฎหมาย แต่ยังช่วยสร้างความเชื่อมั่นให้กับทุกคนในองค์กร

รับขวัญ ชลดำรงคกุล

สารบัญ

บทที่ 1

ที่มาและขอบเขตบังคับใช้ของพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล	21
1.1 ที่มาและเหตุผลของออกประกาศ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	23
1.2 การมีผลบังคับใช้ของพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล	29
1.3 หน่วยงานกำกับดูแลพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล	30
1.4 ขอบเขตการบังคับใช้พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล	31
Q1 : PDPA กำหนดยกเว้นบุคคลหรือหน่วยงานใดบ้าง ? ให้ไม่ต้องปฏิบัติตาม PDPA	32
Q2 : นอกจากบุคคลหรือนิติบุคคลที่ได้รับยกเว้น PDPA นี้ ใช้บังคับกับใครบ้าง ?	39
สรุปท้ายบท	42

unt 2

นินยาศัพททที่สาคัญภายใต้พระราชบัญญัติค้คุมครอง	45
ข้อมูลส่วนบุคคล	
2.1 ข้อมูลส่วนบุคคล	46
Q1 : ภายใต้ PDPA ข้อมูลที่จะถือเป็นข้อมูลส่วนบุคคล	47
ต้องมี้ลักษณะอย่งไร ?	
Q2 : ภายใต้ PDPA ข้อมูลส่วนบุคคลทที่มีควมอ่อนไหว	52
และต้องระม้ดระวังเป็นพิเศษ คีข้อมูลใด ?	
2.2 การประมวผลข้อมูลส่วนบุคคล	56
Q1 : ภายใต้นินยาศของ PDPA ทที่จะถือเป็นการประมวผล	57
ข้อมูลส่วนบุคคล คีการดำนินการใดบ้าง ?	
Q2 : ข้อมูลส่วนบุคคลทได้เก็บไว้ก่อน PDPA	59
มี้ผลบ้งค้บใช้ ผู้ใช้ข้อมูลจะต้องดำนินการอย่งไร ?	
2.3 ผู้ควบค้มข้อมูลส่วนบุคคล	62
และผู้ประมวผลข้อมูลส่วนบุคคล	
Q1 : ภายใต้ PDPA ผู้ควบค้มข้อมูลส่วนบุคคลคีอใคร ?	62
Q2 : ภายใต้ PDPA ผู้ประมวผลข้อมูลส่วนบุคคลคีอใคร ?	64
Q3 : องค์กรหนึ่งสมารถเป็นท้้งผู้ควบค้มข้อมูลส่วนบุคคล	66
และผู้ประมวผลข้อมูลส่วนบุคคลได้หรือไม้ ?	
2.4 เจ้าหน้ทที่ค้คุมครองข้อมูลส่วนบุคคล	67
Q1 : ภายใต้ PDPA เจ้าหน้ทที่ค้คุมครอง	68
ข้อมูลส่วนบุคคลคีอใคร ?	
สรุปท้ยบท	72

บทที่ 3

สรุปหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลภายใต้ PDPA	75
3.1 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	77
Q1 : ภายใต้ PDPA หน้าที่หลักที่กำหนดเฉพาะ ให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลมีอะไรบ้าง ?	77
Q2 : การประมวลผลข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลที่ถูกต้องตาม PDPA ต้องทำอย่างไร ?	85
Q3 : การประเมินว่าวัตถุประสงค์ใดชอบด้วยกฎหมาย ภายใต้ PDPA ต้องพิจารณาอย่างไร ?	86
Q4 : กรณีการประมวลผลข้อมูลส่วนบุคคล มาตรา 26 PDPA กำหนดกรอบความชอบด้วยกฎหมาย ที่แตกต่างไปหรือไม่ ?	98
Q5 : ภายใต้ PDPA ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งอะไรให้เจ้าของข้อมูลส่วนบุคคลทราบบ้าง ?	109
Q6 : Privacy Notice vs Privacy Policy แตกต่างกันอย่างไร ?	115
Q7 : แต่ละองค์กรผู้ควบคุมข้อมูลส่วนบุคคล ต้องมี Privacy Notice กี่ฉบับ ?	128
Q8 : กรณีจำเป็นต้องขอความยินยอม ต้องดำเนินการอย่างไร ? จึงจะถูกต้องตาม PDPA	130

Q9 : สรุปหน้าที่ที่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องปฏิบัติตามเพื่อการประมวลผลข้อมูลส่วนบุคคล ภายใต้ PDPA	135
3.2 โทษและความเสี่ยงของการไม่ปฏิบัติตาม PDPA	138
สรุปท้ายบท	143

บทที่ 4

ภาพรวมการประมวลผลข้อมูลส่วนบุคคล ในการบริหารจัดการทรัพยากรบุคคล	145
4.1 ภาพรวมการประมวลผลข้อมูลส่วนบุคคล	146
4.2 โครงสร้างเนื้อหาของหนังสือเล่มนี้ เพื่อการปรับใช้ในการบริหารจัดการงานทรัพยากรบุคคล	151

บทที่ 5

การคุ้มครองข้อมูลส่วนบุคคลในขั้นตอนการรับสมัครงาน	153
5.1 แหล่งที่มาของข้อมูล	155
Q1 : กรณีมีบุคคลส่งข้อมูล CV เข้ามาสมัครงาน โดยไม่ได้เปิดรับสมัคร ภายใต้ PDPA ต้องดำเนินการอย่างไร ? หรือไม่ ?	155
Q2 : การได้รับข้อมูลผู้สมัครงานมาจาก Job Platform ในแง่ PDPA มีประเด็นต้องกังวลหรือไม่ ?	157

Q3 : เพื่อให้ถูกต้องตาม PDPA	159
การใช้บริการ Headhunter ควรต้องดำเนินการอย่างไร ?	
Q4 : ภายใต้ PDPA การติดต่อผู้สมัครงาน	161
ผ่าน LinkedIn โดยตรง สามารถทำได้หรือไม่?	
5.2 ข้อมูลส่วนบุคคลที่จะมีการประมวลผล	163
Q1 : ภายใต้ PDPA การเก็บข้อมูลส่วนบุคคล	164
เกี่ยวกับคุณสมบัติของผู้สมัครงาน	
จะทำได้มากหรือน้อยเพียงใด ?	
Q2 : ภายใต้ PDPA การเก็บข้อมูลส่วนบุคคล	171
ของบุคคลในครอบครัวของผู้สมัครงาน	
สามารถทำได้หรือไม่ ?	
Q3 : ภายใต้ PDPA การเก็บข้อมูลบัตรประจำตัวประชาชน	173
ของผู้สมัครงาน ควรต้องทำอะไร ?	
Q4 : ภายใต้ PDPA หากองค์กรนายจ้างมีข้อจำกัด	176
การรับสมัครงานที่อ้างอิงจากศาสนา	
ควรต้องทำอะไร ?	
Q5 : ภายใต้ PDPA การเก็บข้อมูลสุขภาพ	179
โดยเฉพาะการตรวจสุขภาพก่อนเข้างาน	
ควรต้องทำอะไร ?	
Q6 : ภายใต้ PDPA การเก็บข้อมูลประวัติอาชญากรรม	182
ในขั้นตอนการรับสมัครงาน ควรต้องทำอะไร ?	
Q7 : ภายใต้ PDPA การเก็บและขอข้อมูลผู้สมัครงาน	186
จากองค์กรนายจ้างเดิมหรือผู้อ้างอิง	
ควรต้องทำอะไร ?	

5.3	วัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล	188
Q1:	วัตถุประสงค์ทั่วไปที่สามารถใช้ เพื่อการประมวลผลข้อมูลส่วนบุคคลของผู้สมัครงาน ได้มีอะไรบ้าง ?	189
Q2 :	ภายใต้ PDPA ในการประมวลผลข้อมูลส่วนบุคคล ของผู้สมัครงานเพื่อจุดประสงค์อื่น ควรต้องดำเนินการอย่างไร ?	191
Q3:	การเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงาน ภายในองค์กรให้แก่ Line Manager มีประเด็นภายใต้ PDPA หรือไม่ ?	195
Q4:	การเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงาน ออกไปนอกองค์กร ให้ถูกต้องตาม PDPA ต้องทำอย่างไร ?	197
Q5 :	ข้อมูลส่วนบุคคลของผู้สมัครงาน หากผ่านการคัดเลือกภายใต้หลักการของ PDPA ควรต้องดำเนินการอย่างไร ?	200
Q6 :	ข้อมูลส่วนบุคคลของผู้สมัครงาน ที่ไม่ผ่านการคัดเลือกภายใต้หลักการของ PDPA ควรต้องดำเนินการอย่างไร ?	201
Q7 :	PDPA กำหนดจำกัดระยะเวลา ในการเก็บรักษาข้อมูลส่วนบุคคล ของผู้สมัครงานไว้อย่างไร ? หรือไม่ ?	203
5.4	เอกสารที่ต้องจัดเตรียมและขั้นตอนการดำเนินการ เพื่อให้ถูกต้องตาม PDPA	205
	สรุปท้ายบท	211

บทที่ 6

การคุ้มครองข้อมูลส่วนบุคคลระหว่าง และหลังสิ้นสุดสัญญาจ้างแรงงาน	213
6.1 ข้อมูลส่วนบุคคลที่จะมีการประมวลผล	215
Q1: ภายใต้ PDPA ข้อมูลสำหรับการ on-board พนักงานที่สามารถเก็บได้คืออะไรบ้าง ?	216
Q2 : ภายใต้ PDPA การเก็บข้อมูลส่วนบุคคลของบุคคล ที่เกี่ยวข้องของพนักงาน สามารถทำได้หรือไม่ ?	222
Q3 : กรณีองค์กรนายจ้างจัดให้มีสวัสดิการ ตรวจสุขภาพประจำปี ภายใต้ PDPA องค์กรนายจ้าง ควรดำเนินการอย่างไร ?	226
Q4 : กรณีองค์กรนายจ้างต้องเก็บลายนิ้วมือ หรือบันทึกใบหน้าของพนักงาน ภายใต้ PDPA ต้องดำเนินการอย่างไร ?	228
Q5 : ภายใต้ PDPA การติดกล้องวงจรปิด ภายในพื้นที่ทำงานขององค์กรนายจ้าง ต้องดำเนินการอย่างไร ?	231
Q6 : ภายใต้ PDPA องค์กรนายจ้าง สามารถเก็บรวบรวมข้อมูลพฤติกรรม Performance ของพนักงานได้เพียงใด ?	232
Q7 : ภายใต้ PDPA การเก็บใบรับรองแพทย์ กรณีลาป่วยเกิน 3 วันทำได้หรือไม่	233

Q8 : ภายใต PDPA การเก็บภาพถ่ายของพนักงาน ในกรณีต่าง ๆ ต้องระมัดระวังอะไรเพิ่มเติมหรือไม่?	235
Q9 : ภายใต PDPA การเก็บข้อมูลในแบบฟอร์มอื่น ๆ ระหว่างการจ้างงานควรต้องระมัดระวัง อะไรเพิ่มเติมหรือไม่ ?	239
6.2 การประมวลผลข้อมูลส่วนบุคคล	240
Q1: วัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล ในฐานะนายจ้าง-ลูกจ้างโดยทั่วไป ที่สามารถทำได้มีอะไรบ้าง ?	242
Q2 : องค์กรนายจ้างสามารถประมวลผลข้อมูลส่วนบุคคล เพื่อประโยชน์ในการดำเนินธุรกิจของตนฝ่ายเดียวได้ หรือไม่ ?	247
Q3 : การเปิดเผยข้อมูลส่วนบุคคลของพนักงาน ภายในองค์กรให้ถูกต้องตาม PDPA ต้องทำอะไร ?	250
Q4 : การเปิดเผยข้อมูลส่วนบุคคล ของพนักงานออกไปนอกองค์กรให้ถูกต้องตาม PDPA ต้องทำอะไร ?	253
6.3 การประมวลผลข้อมูลส่วนบุคคลของอดีตพนักงาน	259
Q1 : การประมวลผลข้อมูลส่วนบุคคลของอดีตพนักงาน ที่สามารถดำเนินการได้ภายใต PDPA มีอะไรบ้าง ?	259
Q2 : ภายใตกรอบ PDPA การเปิดเผยข้อมูลส่วนบุคคล ของอดีตพนักงานทำได้หรือไม่ ? อย่างไร ?	264
Q3 : PDPA กำหนดจำกัดระยะเวลาในการเก็บรักษา ข้อมูลส่วนบุคคลของพนักงานไว้อย่างไร ? หรือไม่ ?	266

6.4 เอกสารที่ต้องจัดเตรียมและขั้นตอนการดำเนินการ	267
เพื่อให้ถูกต้องตาม PDPA มีอะไรบ้าง ?	
สรุปท้ายบท	277

บทที่ 7

การคุ้มครองข้อมูลส่วนบุคคลพนักงาน	279
นอกสัญญาจ้างแรงงาน	
7.1 ความแตกต่างระหว่างการประมวลผล	281
ข้อมูลส่วนบุคคลพนักงานนอกและในสัญญาจ้างแรงงาน	
7.2 ภาพรวมการประมวลผลข้อมูล	283
ส่วนบุคคลพนักงานนอกสัญญาจ้างแรงงาน	
Q1 : ข้อมูลส่วนบุคคลที่จะมีการประมวลผล	284
สำหรับพนักงานนอกสัญญาจ้างแรงงาน	
Q2 : ภายใต้ PDPA การเก็บข้อมูลส่วนบุคคลอันใด	286
ของพนักงานนอกสัญญาจ้างแรงงาน	
ควรดำเนินการอย่างไร ?	
Q3 : ภายใต้ PDPA วัตถุประสงค์และฐานการประมวลผล	288
ข้อมูลส่วนบุคคลของพนักงานนอกสัญญาจ้างแรงงาน	
มีหลักการอย่างไร ?	
Q4 : การเปิดเผยข้อมูลส่วนบุคคล	294
ของพนักงานนอกสัญญาจ้างแรงงานออกไปนอกองค์กร	
ตามหลักการของ PDPA ต้องทำอย่างไร ?	

7.3 การประมวลผลข้อมูลส่วนบุคคลของนักศึกษาฝึกงาน	294
Q1 : เพื่อให้ถูกต้องตาม PDPA องค์กรนายจ้าง	295
ต้องดำเนินการประมวลผลข้อมูลส่วนบุคคล	
นักศึกษาฝึกงานอย่างไร ?	
Q2 : เอกสารและรูปแบบการประกาศการประมวลผล	298
ข้อมูลส่วนบุคคลนักศึกษาฝึกงาน	
ต้องดำเนินการอย่างไร ?	
7.4 การประมวลผลข้อมูลส่วนบุคคลของคู่ค้า (Vendor)	306
Q1 : การประมวลผลข้อมูลส่วนบุคคลผู้ส่งของสินค้า	306
หรือให้บริการภายนอกให้ถูกต้องตาม PDPA	
มีแนวทางอย่างไร ?	
Q2 : การว่าจ้างผู้ประกอบการวิชาชีพอิสระ	309
หรือ Consultant ภายใต้ PDPA มีประเด็นอะไร	
ที่ต้องระมัดระวัง หรือไม่ ?	
Q3 : เอกสารและรูปแบบการประกาศการประมวลผล	312
ข้อมูลส่วนบุคคลคู่ค้าขององค์กรดังกล่าว	
มีรายละเอียดอย่างไร ?	
7.5 การจ้างพนักงาน	322
ผ่านบริษัทรับเหมา Outsourced Manpower	
Q1 : สถานะภายใต้กรอบกฎหมาย PDPA	323
ขององค์กรนายจ้างและบริษัทผู้ให้บริการรับเหมา	
มีรายละเอียดอย่างไร ?	

Q2 : เอกสารและรูปแบบการประกาศการประมวลผล ข้อมูลส่วนบุคคลของพนักงาน ภายใต้บริษัทรับเหมาบริการ มีรายละเอียดอย่างไร ?	327
สรุปท้ายบท	332

บทที่ 8

การคุ้มครองข้อมูลส่วนบุคคล	335
ในกระบวนการบริหารจัดการทรัพยากรบุคคลและองค์กร	
8.1 การจัดทำสัญญา การฝึกอบรมพนักงาน และการกำหนดมาตรการลงโทษ	336
Q1 : ภายใต้ PDPA การทำสัญญาจ้างแรงงาน ต้องเปลี่ยนแปลงอย่างไร ? หรือไม่ ?	337
Q2 : ภายใต้ PDPA การทำสัญญาค้ำประกัน การทำงานต้องเปลี่ยนแปลงอย่างไร ? หรือไม่ ?	342
Q3 : ภายใต้กรอบ PDPA การฝึกอบรมพนักงาน มีความสำคัญอย่างไร ?	345
Q4 : การฝึกอบรมด้าน PDPA สำหรับพนักงานในองค์กร ควรดำเนินการอย่างไร ?	347
Q5 : กลไกการลงโทษวินัยเกี่ยวกับการปฏิบัติตาม PDPA ควรดำเนินการอย่างไร	350
8.2 การจัดโครงสร้างองค์กรภายใต้ PDPA	352
Q1 : คุณสมบัติของ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” ภายใต้ PDPA ประกอบด้วยอะไรบ้าง ?	353

Q2 : ใครในองค์กรควรได้รับการแต่งตั้งเป็น “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” ?	355
Q3 : กระบวนการในการแต่งตั้งเจ้าหน้าที่คุ้มครอง ข้อมูลส่วนบุคคลต้องทำอะไร ?	364
8.3 การลบหรือทำลายข้อมูลส่วนบุคคล	371
8.4 ประเด็นเกี่ยวกับการส่งต่อเปิดเผยข้อมูลส่วนบุคคล ภายนอกองค์กร	376
Q1 : กรณีการส่งต่อเปิดเผยข้อมูลส่วนบุคคล ออกไปนอกองค์กร มีข้อควรปฏิบัติ ภายใต้ PDPA อย่างไร ?	377
Q2 : กรณีที่มีการจัดทำสัญญาการรักษาความลับอยู่แล้ว ยังต้องทำสัญญาการประมวลผลข้อมูลส่วนบุคคล อีกหรือไม่ ?	393
Q3 : ภายใต้ PDPA กรณีที่กลุ่มบริษัทใช้ Shared HR Resources ร่วมกัน มีข้อควรปฏิบัติ หรือข้อควรระมัดระวังอย่างไร ?	402
Q4 : ภายใต้ PDPA กรณีการประมวลผลข้อมูลส่วนบุคคล โดย Thai Subsidiary ของ Global HQ มีข้อควรระมัดระวังใดบ้าง ?	410
สรุปท้ายบท	413

unที่ 9

มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล	415
และการบริหารจัดการ Data Breach	
9.1 หน้าที่การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล	417
Q1 : ความมั่นคงปลอดภัย	417
ของข้อมูลส่วนบุคคลหมายถึงอะไร ?	
Q2 : การรักษาความมั่นคงปลอดภัย	418
รวมเฉพาะข้อมูลที่เก็บในระบบเทคโนโลยีสารสนเทศ	
ใช้หรือไม่ ?	
Q3 : มาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ	421
และเหมาะสม ประเมินจากอะไร ?	
Q4 : Checklist ขั้นต่ำที่คณะกรรมการฯ คาดหวัง	424
สำหรับการรักษาความมั่นคงปลอดภัยข้อมูลมีอะไรบ้าง ?	
Q5 : มาตรการรักษาความมั่นคงปลอดภัยข้อมูล	429
ต้องได้รับการทบทวนหรือไม่ ? อย่างไร ?	
Q6 : มาตรการรักษาความมั่นคงปลอดภัย	430
ต้องใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่	
อย่างไร	
Q7 : จำเป็นต้องมีนโยบายรักษาความมั่นคงปลอดภัย	432
ข้อมูลส่วนบุคคลขึ้นเป็นการเฉพาะหรือไม่ ?	
9.2 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	439
Q1 : กลไกการบริหารจัดการเหตุการณ์	440
ละเมิดข้อมูลส่วนบุคคลควรดำเนินการอย่างไร ?	

Q2 : กลไกการแจ้งเหตุและการรายงาน เหตุการณ์ละเมิดข้อมูลส่วนบุคคล ควรดำเนินการอย่างไร ?	442
Q3 : ข้อมูลที่ต้องรายงานไปยังสำนักงานฯ กรณีเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมีอะไรบ้าง	454
Q4 : ผู้ควบคุมข้อมูลส่วนบุคคล ต้องรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ไปยังเจ้าของข้อมูลส่วนบุคคลหรือไม่ ?	457
สรุปท้ายบท	462

บทที่ 10

สิทธิเจ้าของข้อมูลส่วนบุคคล	465
และการตอบรับการใช้สิทธิเจ้าของข้อมูลส่วนบุคคล	
10.1 สิทธิที่เจ้าของข้อมูลส่วนบุคคลมีภายใต้ PDPA และสิทธิของผู้ควบคุมข้อมูลส่วนบุคคลในการปฏิเสธ	466
10.2 กระบวนการและกลไกในการขอใช้สิทธิ ของเจ้าของข้อมูล	475
สรุปท้ายบท	485

บทที่ 11

Final Checkpoints	487
--------------------------	------------



บทที่ 01

ที่มาและขอบเขตบังคับใช้
ของพระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล

ก่อนที่จะทำความเข้าใจเกี่ยวกับเนื้อหาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) การทำความเข้าใจถึงที่มาที่ไปและเหตุผลของการออกพระราชบัญญัตินี้ดังกล่าว เป็นส่วนสำคัญจะช่วยให้ผู้ประกอบการที่มีหน้าที่ต้องปฏิบัติตามกฎหมายฉบับดังกล่าวเข้าใจ **“จุดประสงค์และเป้าหมาย” (Objectives & Purposes)** ที่พระราชบัญญัติฉบับนี้ต้องการบรรลุ ซึ่งความเข้าใจจะช่วยให้ผู้ประกอบการสามารถตั้งเป้าใช้จุดประสงค์ดังกล่าวเป็นหลักการในการตีความการใช้และการปฏิบัติตามพระราชบัญญัติได้อย่างสมบูรณ์

นอกจากนี้ ก่อนที่จะทำความเข้าใจการบังคับใช้กฎหมาย โดยเฉพาะในส่วนของการประมวลผลข้อมูลส่วนบุคคลในงานบริหารจัดการทรัพยากรบุคคล ซึ่งเป็นกระบวนการทำงานและการใช้ข้อมูล (Data Flow) ที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างมากและเป็นหัวข้อหลักของหนังสือฉบับนี้ ความเข้าใจเกี่ยวกับภาพรวมของกฎหมาย ขอบเขตบังคับใช้ของพระราชบัญญัตินี้ดังกล่าวในภาพใหญ่ของการทำงานขององค์กรจึงเป็นสิ่งสำคัญ

1.1 ที่มาและเหตุผลของออกประกาศ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ประเทศไทยจำเป็นต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่มีมาตรฐานเท่าต่างประเทศ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ได้รับการประกาศกำหนดขึ้นตั้งแต่ปี พ.ศ. 2562 เพื่อให้สอดคล้องกับการปรับตัวทางด้านกฎหมายทั่วโลกที่ให้ความสำคัญกับความเป็นส่วนตัว (Privacy) และสิทธิความเป็นเจ้าของข้อมูลส่วนบุคคล (Rights to Personal Data) ของบุคคลต่าง ๆ โดยเฉพาะให้สอดคล้องได้มาตรฐานภายใต้กรอบกฎหมายของสหภาพยุโรปที่มีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นต้นแบบของหลาย ๆ ประเทศทั่วโลก ได้แก่ General Data Protection Regulations (GDPR) ซึ่งเป็นกรอบกฎหมายที่ได้รับการปรับปรุงขึ้นมาให้มีผลบังคับโดยสมบูรณ์เพื่อปกป้องสิทธิเหนือข้อมูลส่วนบุคคลของประชากรยุโรป ไม่ว่าจะถูกนำไปใช้ประมวลผลอยู่ที่ใดในโลกก็ตาม ตั้งแต่ปี พ.ศ. 2559

การมีผลบังคับใช้ของ GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศต่าง ๆ ในโลก เป็นหนึ่งในเหตุผลหลักที่ประเทศไทยจำเป็นต้องมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างเร่งด่วน เพราะกรอบกฎหมายของประเทศต่าง ๆ กำหนดว่า หากจะมีการส่งข้อมูลที่ถือเป็นข้อมูลส่วนบุคคลออกนอกประเทศของตนไปยังประเทศอื่น ประเทศปลายทางจำเป็นต้องมีกรอบกฎหมายที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ในลักษณะที่ใกล้เคียง

ได้มาตรฐานเดียวกับประเทศต้นทางที่จะมีการส่งข้อมูลออกไป ดังนั้น หากประเทศไทยยังไม่มีกรอบกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐาน ประเทศไทยจะไม่สามารถ “รับข้อมูลส่วนบุคคล” จากประเทศอื่น ๆ ที่มีกรอบกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เลย และในโลกที่มีการส่งต่อข้อมูลระหว่างกันอย่างรวดเร็วหมด หากประเทศไทยไม่สามารถรับข้อมูลจากประเทศอื่นได้ ย่อมกระทบต่อความสามารถในการแข่งขันและการดำเนินธุรกิจของประเทศในหลาย ๆ ด้าน ประเทศไทยจึงจำเป็นต้องเร่งในการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมาในปี พ.ศ. 2562

กฎหมายที่คุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ก่อนจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ก่อนการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเป็นการเฉพาะ ประชาชนไทยก็ได้รับการคุ้มครองสิทธิความเป็นส่วนตัวและสิทธิเหนือข้อมูลส่วนบุคคลของตนเช่นกัน แต่เป็นการคุ้มครองภายใต้กรอบกฎหมายทั่วไป ได้แก่ **รัฐธรรมนูญ ประมวลกฎหมายแพ่ง และพาณิชย์ และกฎหมายอาญา** หรืออาจรวมถึงกฎหมายอื่น ๆ ซึ่งอาจกล่าวถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลอยู่บางส่วน โดยเฉพาะในส่วนของการประมวลผลข้อมูลที่มีความอ่อนไหวสูง แต่ไม่ได้เป็นการคุ้มครองโดยเฉพาะทั้งฉบับ

การคุ้มครองสิทธิภายใต้กรอบการฟ้องคดีตามกฎหมายแพ่งและพาณิชย์ : โดยหลักเป็นการใช้สิทธิภายใต้กรอบการฟ้องคดี “ละเมิด” โดยหากบุคคลใดได้รับผลกระทบเกิดความเสียหายต่อสิทธิไม่ว่าในลักษณะใด (เช่น สิทธิความเป็นส่วนตัวหรือชื่อเสียง)

อันเกิดจากการกระทำของบุคคลอื่นไม่ว่าจงใจหรือประมาทเลินเล่อ บุคคลที่ได้รับความเสียหายสามารถเรียกค่าสินไหมทดแทนจากบุคคล ผู้กระทำการละเมิดได้ แต่ในการคุ้มครองสิทธิภายใต้หลักการละเมิดนี้ มีปัญหาในทางปฏิบัติ คือ ภายใต้กรอบกฎหมายละเมิด **ผู้มีหน้าที่ ในการพิสูจน์การกระทำผิด (Burden of Proof) คือ ผู้ฟ้องร้อง** ซึ่งการพิสูจน์การกระทำละเมิดข้อมูลในโลกปัจจุบันที่มีการใช้เทคโนโลยี ที่ซับซ้อนมากขึ้น ย่อมเป็นเรื่องยากและเป็นภาระอย่างมากสำหรับ ผู้ฟ้องร้องในการพิสูจน์ข้อความผิดเกี่ยวกับการใช้ข้อมูลดังกล่าวต่อศาล

การคุ้มครองสิทธิภายใต้กรอบการฟ้องคดีตามกฎหมายอาญา : ไม่มีข้อบัญญัติใดในกฎหมายที่คุ้มครองความผิดเกี่ยวกับ “ข้อมูล ส่วนบุคคล” โดยตรง มีเพียงกรอบกฎหมายทั่วไปที่อาจนำมาปรับ ใช้กับการณีการใช้ข้อมูลได้หากครบ “องค์ประกอบความผิด” ตามที่กฎหมายกำหนด เช่น กรณีการขโมยข้อมูลสามารถฟ้องร้อง ได้แบบ “คดีลักทรัพย์” การใช้ข้อมูลส่วนบุคคลและนำไปหลอกลวง ก็เป็นการฟ้องร้อง “คดีฉ้อโกง” ซึ่งเป็นส่วนความผิดที่ต่อเนื่อง ไม่ใช่ ความรับผิดจากการใช้ข้อมูลในส่วนแรกโดยตรง หรือกรณีการใช้ข้อมูล ไปสร้าง ความรำคาญก็เป็นการฟ้องร้องภายใต้กรอบ “คดีสร้าง ความรำคาญ” ซึ่งเป็นลหุโทษที่ยอมความกันได้ โทษไม่สูง ซึ่งจะเห็น ได้ว่าการฟ้องร้องคุ้มครองสิทธิภายใต้กรอบกฎหมายอาญาทั่วไปนั้น มีข้อจำกัดค่อนข้างมาก ทั้งในแง่ของความผิดที่ไม่ได้มีการคุ้มครอง โดยตรง การพิสูจน์ความเสียหายที่เป็นของผู้ฟ้องร้อง และการรับผิดชอบ ทางด้านอาญา กรณีเป็นการดำเนินการของนิติบุคคลอาจไม่สามารถ พิสูจน์ความรับผิดไปถึงตัวนิติบุคคลที่เกี่ยวข้องได้ เป็นเพียง ความรับผิดของปัจเจกชนเท่านั้น ทำให้การกระทำผิดทางอาญา

เป็นเรื่องเฉพาะบุคคลมากกว่าจะเป็นกรอบความผิดที่ครอบคลุมไปถึงองค์กรต้นสังกัด

กฎหมายเฉพาะอื่น : อาทิ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 สำหรับการประมวลผลข้อมูลส่วนบุคคล ภาครัฐหรือระเบียบกระทรวงสาธารณสุข เรื่อง การคุ้มครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 โดยหลักการกฎหมายดังกล่าวทำหน้าที่เพื่อกำหนดกรอบการใช้ข้อมูลส่วนบุคคล โดยหน่วยงานบางหน่วยงานเป็นการเฉพาะเท่านั้น แต่ไม่ได้ให้การคุ้มครองสิทธิแก่ผู้เป็นเจ้าของข้อมูลส่วนบุคคลโดยตรง

การออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นเป็นการเฉพาะ ช่วยแก้ไขปัญหาคำจำกัดภายใต้กฎหมายทั่วไปเดิม

ด้วยปัจจัยความเร่งด่วนที่ประเทศไทยต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ได้มาตรฐานเท่ากับต่างประเทศ และด้วยปัญหาการบังคับใช้กฎหมายทั่วไปกับการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่วิเคราะห์ไว้ข้างต้น จึงมีความจำเป็นอย่างมากสำหรับประเทศไทยในการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นในปี พ.ศ. 2562

ทั้งนี้ ในการอ่านและทำความเข้าใจกฎหมายฉบับหนึ่ง เราสามารถศึกษาทำความเข้าใจ “เจตจำนง” ของการมีของกฎหมายนั้นได้จากเหตุผลที่ระบุไว้ในหมายเหตุท้ายกฎหมายแต่ละฉบับ ซึ่งการทำความเข้าใจเหตุผลการออกดังกล่าวจะช่วยสร้าง “หลัก” ในการตีความการใช้กฎหมายได้อย่างดี และสำหรับการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ หมายเหตุตอนท้ายกำหนด

ว่าเหตุผลในการประกาศกฎหมายคือ “เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อน รำคาญ หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป”

ดังนั้น จะเห็นได้ว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้รับการประกาศกำหนดขึ้นมาเพื่อ (ก) คุ้มครองสิทธิของเจ้าของข้อมูล และ (ข) กำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ที่ต้องการใช้ข้อมูลส่วนบุคคลของบุคคลอื่นเป็นสำคัญ โดยมีจุดประสงค์เป็นกฎหมายทั่วไปที่ใช้บังคับสำหรับการประมวลผลข้อมูลส่วนบุคคล

การกำหนดกรอบการเป็นกฎหมายทั่วไปที่มีผลควบคุมคุ้มครองการประมวลผลข้อมูลส่วนบุคคล (ซึ่งเป็นประเด็นหลักหรือ Subject Matter หลักของกฎหมายฉบับนี้) หมายความว่า ในการตีความกฎหมายว่ากฎหมายใดจะมีผลบังคับในกรณีใดนั้น หากเป็นเรื่องใดก็ตามที่เกี่ยวข้องเนื่องกับการประมวลผลข้อมูลส่วนบุคคล พระราชบัญญัติฉบับนี้จะถูกใช้เป็นกฎหมายหลักก่อน

แต่ทั้งนี้ ภายใต้มาตรา 3 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดชัดเจนไว้ว่า หากมีกฎหมายอื่นที่มีบทบัญญัติ

เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะกิจการหรือหน่วยงานใด โดยเฉพาะแล้ว ให้บังคับตามกฎหมายเฉพาะนั้น เว้นแต่

(ก) บทบัญญัติเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล บทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงบทกำหนดโทษที่เกี่ยวข้อง และ

(ข) บทบัญญัติเกี่ยวกับการร้องเรียนที่ให้อำนาจของคณะกรรมการผู้เชี่ยวชาญในการออกคำสั่ง ให้เป็นตามบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลทั้งหมด ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม โดยเฉพาะกรณีที่เจ้าหน้าที่ผู้มีอำนาจตามกฎหมายเฉพาะดังกล่าวไม่มีอำนาจเพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญ

ภายใต้รูปแบบและหลักการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงกลายเป็นกฎหมายที่สร้าง “เสาหลัก” สำหรับการคุ้มครองสิทธิเจ้าของข้อมูลส่วนบุคคล และกำกับการประมวลผลข้อมูลส่วนบุคคลโดยบุคคลใด ๆ ก็ตามให้เป็นมาตรฐาน แต่อย่างไรก็ตาม พระราชบัญญัตินี้ ไม่ได้มีจุดประสงค์ สร้างขึ้นเพื่อเปลี่ยนแปลงหรือลบล้างกฎหมายอื่นที่มีผลบังคับใช้เพื่อทำหน้าที่และกลไกการคุ้มครองและกำกับ แต่เป็นไปในลักษณะของการเสริมแรงให้มีความเข้มแข็งขึ้นมากกว่า ผู้ประกอบการที่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลของบุคคลใดก็ตาม จึงต้องให้ความสำคัญและสนใจทั้งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายเฉพาะอื่นที่อาจเกี่ยวข้อง

1.2 การมีผลบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะมีการประกาศใช้ตั้งแต่ปี พ.ศ. 2562 แต่ด้วยเหตุที่พระราชบัญญัตินี้ดังกล่าวมีผลบังคับใช้อย่างกว้างขวางและเป็นกฎหมายฉบับใหม่ ต้องอาศัยการสร้างความเข้าใจเกี่ยวกับการปรับใช้และการปฏิบัติตามกฎหมายของทุกภาคส่วน มาตรา 2 ของพระราชบัญญัติกำหนดชัดเจนว่าพระราชบัญญัตินี้มีผลบังคับใช้เพียงบางมาตราจะมีผลบังคับใช้นับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา (วันที่ 28 พฤษภาคม พ.ศ. 2562) แต่บทบัญญัติส่วนมาก โดยเฉพาะส่วนที่เป็นหลักคือการกำหนดการประมวลผลข้อมูล การคุ้มครองสิทธิเจ้าของข้อมูล รวมถึงโทษต่างๆ จะมีผลบังคับใช้เมื่อพ้นกำหนดในอีก 1 ปี (วันที่ 27 พฤษภาคม พ.ศ. 2563) แต่ด้วยความไม่พร้อม มีการออกพระราชกำหนดขยายระยะเวลาการมีผลบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวออกไปอีกถึง 2 ครั้ง โดยให้มีผลบังคับสมบูรณ์ทั้งฉบับในวันที่ 1 มิถุนายน พ.ศ. 2565

กฎหมายลำดับรองที่ออกภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

นอกจากพระราชบัญญัติหลักที่มีผลบังคับใช้โดยสมบูรณ์แล้ว ในปัจจุบันได้มีการออกกฎหมายลำดับรองจำนวนมากเพื่อรองรับขยายความเพิ่มเติมบทบัญญัติของพระราชบัญญัตินี้ดังกล่าว ทั้งในรูปแบบ

ของพระราชกฤษฎีกา (พระราชกฤษฎีกากำหนดลักษณะกิจการหรือหน่วยงานที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบางส่วนมาใช้บังคับ) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจำนวน 20 ฉบับ (ทั้งในส่วนที่เกี่ยวข้องกับการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และส่วนที่เกี่ยวข้องโดยตรงกับการกำกับการประมวลผลข้อมูลส่วนบุคคล)

1.3 หน่วยงานกำกับดูแลพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ภายใต้กรอบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีการจัดตั้ง**คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**ขึ้นมาเป็นการเฉพาะ มีหน้าที่และอำนาจกำหนดมาตรการหรือแนวทางดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติ และมีการจัดตั้ง**สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**ขึ้นมาเป็นนิติบุคคลแยก เพื่อปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเป็นศูนย์กลางในการให้บริการทางวิชาการหรือบริการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานของรัฐ หน่วยงานเอกชน และประชาชน

นอกจากโครงสร้างองค์กรหลักที่ทำหน้าที่ในการกำกับดูแลออกนโยบาย และประกาศที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลแล้ว พระราชบัญญัติกำหนดแต่งตั้ง**คณะกรรมการ**

ผู้เชี่ยวชาญเพื่อทำหน้าที่ในการพิจารณารับเรื่องร้องเรียนตามพระราชบัญญัติ ตรวจสอบการกระทำของบุคคลที่ก่อให้เกิดความเสียหาย รวมถึงออกคำสั่งให้ดำเนินการหรือดเว้นการดำเนินการ รวมถึงกำหนดโทษปกครองกรณีเกิดการฝ่าฝืนพระราชบัญญัติ ซึ่งปัจจุบันมีคณะกรรมการผู้เชี่ยวชาญทั้งหมด 4 คณะด้วยกัน โดยแบ่งเป็น

- คณะที่ 1 รับเรื่องร้องเรียนเกี่ยวกับการเงินและเศรษฐกิจ
- คณะที่ 2 รับเรื่องร้องเรียนเกี่ยวกับเทคโนโลยีดิจิทัลและอื่น ๆ
- คณะที่ 3 รับเรื่องร้องเรียนเกี่ยวกับหน่วยงานภาครัฐ
- คณะที่ 4 รับเรื่องร้องเรียนด้านสุขภาพและการศึกษาวิจัยหรือสถิติ

1.4 ขอบเขตการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

เมื่อเข้าใจถึงที่มาที่ไป เหตุผลความสำคัญ รวมถึงกรอบการกำกับดูแลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในภาพกว้างแล้ว อีกหัวข้อหลักที่ควรต้องทำความเข้าใจให้ตรงกันคือ ขอบเขตการบังคับใช้พระราชบัญญัตินี้ ซึ่งระบุไว้เป็นกรอบที่ชัดเจนภายใต้มาตรา 4 และมาตรา 5 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือเรียกย่อ ๆ ว่า PDPA

Q1 : PDPA กำหนดยกเว้นบุคคลหรือหน่วยงานใดบ้าง ?

ให้ไม่ต้องปฏิบัติตาม PDPA

มาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดชัดเจนว่าพระราชบัญญัติฉบับนี้จะไม่ใช้บังคับแก่

1. การประมวลผลข้อมูลที่เป็นเรื่องส่วนตัว การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ดำเนินการเพื่อประโยชน์ส่วนตัวหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น **ได้รับการยกเว้นจากการบังคับภายใต้พระราชบัญญัติฉบับนี้ทั้งฉบับ** แปลว่าหาก**บุคคลธรรมดา**คนหนึ่งทำการเก็บรวบรวม ใช้ หรือแม้กระทั่งเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นไม่ว่าในลักษณะใด หากเป็นการดำเนินการแบบส่วนตัว เช่น การถ่ายรูป Selfie หรือการถ่ายภาพ Street ใด ๆ ก็ตาม (การถ่ายภาพ Street คือ การถ่ายภาพผู้คนและสภาพแวดล้อมในชีวิตประจำวันตามสถานที่สาธารณะ) แม้กระทั่งการ Post รูปดังกล่าวลงในช่องทาง Social Media **ส่วนตัวของตนเอง** (ที่จะเป็น Public/Private) บุคคลดังกล่าวไม่มีหน้าที่ต้องดำเนินการใดภายใต้พระราชบัญญัติฉบับนี้เลย และบุคคลใดก็ตามไม่สามารถอ้างสิทธิภายใต้พระราชบัญญัติฉบับนี้ได้ ไม่ว่าจะเป็นสิทธิการขอลบหรือสิทธิการฟ้องร้องใด ๆ แต่หากบุคคลอื่นที่อยู่ในภาพนั้นได้รับความเสียหาย เช่น เป็นภาพที่ไม่ควรได้รับการเผยแพร่และทำให้ความเสียหาย บุคคลนั้นต้องดำเนินการฟ้องร้องภายใต้กรอบกฎหมายทั่วไป เช่น การฟ้องละเมิดภายใต้ประมวลกฎหมายแพ่งและพาณิชย์แทน

2. การดำเนินการของหน่วยงานรัฐ เฉพาะที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งกำหนดเป็นการเฉพาะสำหรับการดำเนินการที่เกี่ยวกับความมั่นคงทางการคลังของรัฐ การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ และการรักษาความมั่นคงปลอดภัยไซเบอร์ ข้อยกเว้นนี้จำกัดเฉพาะหน่วยงานรัฐ และต้องเป็นหน่วยงานรัฐที่ทำหน้าที่เฉพาะส่วนที่ระบุไว้ในพระราชบัญญัติฉบับนี้เท่านั้น เช่น การที่สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงินจำเป็นต้องเก็บรวบรวมข้อมูลของผู้ที่มีความเสี่ยงฟอกเงินหรือต้องเปิดเผยข้อมูลดังกล่าวเพื่อภารกิจหลักของหน่วยงานของตนตามที่ระบุไว้ในกฎหมายสำนักงานฯ สามารถดำเนินการดังกล่าวได้โดยไม่ต้องแจ้งการประมวลผลข้อมูลส่วนบุคคลนั้นแก่บุคคลที่เกี่ยวข้องก่อนหรือขอการเก็บข้อมูล ทั้งนี้ การยกเว้นนี้จำกัดเฉพาะส่วนที่เกี่ยวข้องกับการประมวลผลของข้อมูลส่วนบุคคลที่เป็นส่วนที่หน่วยงานดังกล่าวดำเนินการเพื่อให้ตอบโจทย์เป้าหมายการรักษาความมั่นคงของรัฐเท่านั้น ไม่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลในด้านอื่น นั่นหมายถึงว่ากรณีการบริหารจัดการทรัพยากรบุคคลภายในของหน่วยงานรัฐดังกล่าวยังต้องดำเนินการภายใต้พระราชบัญญัติทั้งหมด

3. การประมวลผลข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรือวรรณกรรม หากบุคคลหรือนิติบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรือวรรณกรรม และดำเนินการดังกล่าวโดยอ้างอิงตามจริยธรรมแห่งการประกอบวิชาชีพหรือดำเนินการเพื่อประโยชน์สาธารณะแล้ว การประมวลผลข้อมูลส่วนบุคคลนั้น

จะได้รับการยกเว้นจากการแจ้งการประมวลผลข้อมูลส่วนบุคคล หรือการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ดังนั้นกรณี นักข่าว (หากได้รับการขึ้นทะเบียนเป็นสื่อมวลชน) ดำเนินการประมวลผล ข้อมูลส่วนบุคคลภายใต้มรรยาทหรือจริยธรรมการเป็นสื่อมวลชนหรือ เป็นการดำเนินการเพื่อประโยชน์ของสาธารณะแล้ว สามารถ เก็บรวบรวมและเปิดเผยข้อมูลส่วนบุคคลของบุคคลในข่าวได้ โดยได้รับการยกเว้นจากหน้าที่บางส่วนภายใต้พระราชบัญญัติ แต่การยกเว้นก็จะเป็นการยกเว้น **จำกัดเฉพาะ** สำหรับส่วนของ การประมวลผลข้อมูลส่วนบุคคลเพื่อการสื่อมวลชนเท่านั้น เช่นเดียวกัน กับหน่วยงานรัฐ กรณีการบริหารจัดการทรัพยากรบุคคลภายใน ของนิติบุคคลที่ดำเนินกิจการสื่อมวลชนยังต้องดำเนินการภายใต้ พระราชบัญญัติทั้งหมด

4. **สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึง คณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว** ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการพิจารณาตามหน้าที่และอำนาจ ของสภาฯ การยกเว้นดังกล่าวใช้เฉพาะสำหรับการประมวลผลข้อมูล ส่วนบุคคลที่เกี่ยวข้องโดยตรงกับการทำหน้าที่ของสภาหรือ คณะกรรมการดังกล่าวเท่านั้น หากสมาชิกสภาหรือสมาชิก คณะกรรมการต่าง ๆ ใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์อื่นที่ไม่ใช่ การทำหน้าที่ บุคคลหรือคณะกรรมการเหล่านั้นย่อมถือเป็น บุคคลผู้มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคลอยู่เช่นเดิม

5. **การพิจารณาคดีและการดำเนินงานในกระบวนการยุติธรรม** พระราชบัญญัติมีจุดประสงค์ยกเว้นการประมวลผลข้อมูลส่วนบุคคล

ในการพิจารณาพิพากษาคดีของศาล กระบวนการพิจารณาคดี บังคับคดี การวางทรัพย์ ทั้งในคดีแพ่งและคดีอาญา ซึ่งเป็นการดำเนินการของศาลและเจ้าหน้าที่ในกระบวนการพิจารณาเป็นหลัก ดังนั้นการยกเว้นนี้เป็นการยกเว้นหน่วยงาน ได้แก่ ศาล อัยการ ตำรวจ เจ้าหน้าที่บังคับคดี หรือเจ้าพนักงานอื่นที่อาจเกี่ยวข้อง ในกระบวนการพิจารณาคดีและอำนวยความสะดวกยุติธรรมเป็นหลัก อาจไม่ได้รวมถึงตัวคดีความที่อาจดำเนินการใด ๆ โดยลำพัง และการยกเว้นภายใต้พระราชบัญญัติดังกล่าว ยกเว้นเฉพาะการประมวลผล ข้อมูลส่วนบุคคลที่เกี่ยวข้องโดยตรงกับการดำเนินกระบวนการยุติธรรม เท่านั้น ไม่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลในด้านอื่น นั้นหมายความว่า **กรณีการบริหารจัดการทรัพยากรบุคคลภายในของ หน่วยงานดังกล่าวยังต้องดำเนินการภายใต้พระราชบัญญัติ ทั้งหมด**

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต พระราชบัญญัติฉบับนี้มีจุดประสงค์ยกเว้นเฉพาะกระบวนการตรวจเครดิตบูโร (Credit Bureau เปรียบเหมือนกับบัตรประจำตัวทางการเงิน ที่รวบรวมข้อมูลการชำระหนี้เชื้อจากสถาบันการเงินต่าง ๆ เพื่อนำมาใช้ประเมินความน่าเชื่อถือทางการเงินของบุคคลนั้น) ที่ดำเนินการโดยตัวบริษัทข้อมูลเครดิตเองและสมาชิกเท่านั้น ไม่ได้มีจุดประสงค์ครอบคลุมไปยังบุคคลอื่นที่อาจได้รับข้อมูลจากบริษัทหรือสมาชิกดังกล่าว ซึ่งยังคงมีหน้าที่เต็มในการปฏิบัติตามพระราชบัญญัติ และการยกเว้นตามพระราชบัญญัติฉบับนี้เป็นการยกเว้นเฉพาะส่วน การประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ภายใต้

พระราชบัญญัติเท่านั้น ไม่ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลในด้านอื่น และเน้นอนกณการบริหารจัดการทรัพยากรบุคคลภายในของหน่วยงานดังกล่าวยังต้องดำเนินการภายใต้พระราชบัญญัติทั้งหมด

7. การประมวลผลข้อมูลส่วนบุคคลอื่นที่ได้รับการยกเว้นภายใต้พระราชกฤษฎีกา มีการประกาศพระราชกฤษฎีกากำหนดลักษณะกิจการหรือหน่วยงานที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566 โดยจำกัดการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล (ทั้งภาครัฐและเอกชน) ที่ประมวลผลข้อมูลส่วนบุคคลเฉพาะกรณีที่กำหนดไว้ ได้แก่

(ก) การประมวลผลข้อมูลส่วนบุคคลที่ได้รับการร้องขอจากคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ หรือหน่วยงานรัฐที่มีอำนาจขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการทุจริต

(ข) การประมวลผลข้อมูลส่วนบุคคลที่ได้รับการร้องขอจากกรมสรรพากร กรมศุลกากร หรือกรมสรรพสามิต ตามกฎหมายที่อยู่ในความรับผิดชอบเกี่ยวกับการจัดการเก็บภาษีอากร

(ค) การประมวลผลข้อมูลส่วนบุคคลที่ได้รับการร้องขอจากองค์กรปกครองส่วนท้องถิ่น ซึ่งอาศัยอำนาจตามกฎหมายเพื่อวัตถุประสงค์และภารกิจการจัดเก็บภาษีตามกฎหมายว่าด้วยภาษีที่ดินและสิ่งปลูกสร้าง

(ง) การประมวลผลข้อมูลส่วนบุคคลที่ได้รับการร้องขอจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจในการขอข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะที่สำคัญตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะประกาศกำหนด

ทั้งนี้ ภายใต้พระราชกฤษฎีกาดังกล่าวเป็นการยกเว้นเฉพาะการปฏิบัติตามหมวด 2 (การคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงการแจ้งการประมวลผลข้อมูล และ/หรือการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล) และหมวด 3 (การใช้หรือเปิดเผยข้อมูลส่วนบุคคล) ของพระราชบัญญัติฯ เท่านั้น นั่นแปลว่า บทบัญญัติอื่น ๆ ของพระราชบัญญัตียังคงมีผลบังคับใช้ โดยเฉพาะพระราชกฤษฎีกาดังกล่าวจะไม่มีผลยกเว้นความผิดและโทษอาญาตามพระราชบัญญัติฯ หากมีการดำเนินการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานที่อาจได้รับการยกเว้น แต่ไม่ชอบด้วยกฎหมายตามกรอบที่กำหนดไว้ในพระราชกฤษฎีกา หน่วยงานดังกล่าวยังคงมีความเสี่ยงต้องรับโทษภายใต้ PDPA ครบถ้วนเช่นเดิม

ประเด็นเพิ่มเติมเกี่ยวกับการยกเว้นการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 4 ที่ทุกหน่วยงานหรือบุคคลที่อยู่ภายใต้การขอการยกเว้นดังกล่าว (ยกเว้นเพียงกรณีของบุคคลธรรมดาที่ประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัวหรือครอบครัว) ต้องพิจารณาและคำนึงถึงคือ ภายใต้มาตรา 4 **ผู้ควบคุมข้อมูลส่วนบุคคลแม้จะอยู่ในกรณีได้รับการยกเว้นการปฏิบัติตามพระราชบัญญัติเป็นส่วนใหญ่ แต่ก็ยังคงต้องมีหน้าที่จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดไว้ในพระราชบัญญัติ** ดังนั้นแม้ว่าหน้าที่หลักข้อหนึ่งที่บุคคล

และหน่วยงานนั้นยังต้องดำเนินการเสมอ คือ การที่ต้องรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ตนเก็บรวบรวม ประมวลผล ใช้ และเปิดเผยให้ได้มาตรฐานที่กำหนดไว้ ซึ่งหากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของตน แปลว่าโทษทางแพ่งหรือโทษทางอาญาภายใต้พระราชบัญญัติจะยังคงมีผลบังคับกับหน่วยงานหรือบุคคลนั้นอยู่เช่นเดิม ไม่ใช่การยกเว้นจากหน้าที่และความรับผิดชอบภายใต้พระราชบัญญัติอย่างสมบูรณ์

ดังนั้นสรุปได้ว่า แม้บางหน่วยงานทั้งที่เป็นภาครัฐและเอกชน อาจได้รับการยกเว้นจากการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางมาตรา โดยเฉพาะส่วนของการแจ้งการประมวลผลข้อมูลส่วนบุคคล หรือการขอความยินยอมการประมวลผลข้อมูลส่วนบุคคล หรือการยกเว้นจากการปฏิบัติหน้าที่บางส่วนในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เช่น การจัดทำบันทึกการการประมวลผลข้อมูลส่วนบุคคลหรือการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แต่

(1) การยกเว้นดังกล่าวเป็นการยกเว้นเฉพาะบางมาตรา หน่วยงานดังกล่าวยังมีหน้าที่ที่ต้องดำเนินการตามพระราชบัญญัติอยู่ โดยเฉพาะการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของตน ซึ่งหากทำหน้าที่ไม่ครบถ้วนยังต้องรับโทษจากการดำเนินการประมวลผลข้อมูลส่วนบุคคลของตนเองอยู่ และ

(2) การยกเว้นนั้นจำกัดเฉพาะในขอบเขตที่เกี่ยวข้องกับการประมวลผลที่ได้รับการกำหนดเฉพาะให้ได้รับการยกเว้นเท่านั้น ไม่ใช่การยกเว้นจากการประมวลผลข้อมูลส่วนบุคคลทุกส่วน ทุก Data Flow ที่หน่วยงานดังกล่าวดำเนินการ โดยเฉพาะอย่างยิ่ง**การประมวลผล**

ข้อมูลส่วนบุคคลของบุคลากรภายในของหน่วยงาน ทุกหน่วยงานดังกล่าวยังมีหน้าที่ต้องประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในทุกส่วนอยู่เช่นเดิม

Q2 : นอกจากบุคคลหรือนิติบุคคลที่ได้รับยกเว้น PDPA นี้
ใช้บังคับกับใครบ้าง ?

PDPA ใช้บังคับตามหลักการการตั้งอยู่ของบุคคลหรือนิติบุคคลที่ประมวลผลข้อมูล : มาตรา 5 ของ PDPA ระบุชัดเจนว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลใช้บังคับแก่การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยบุคคลและนิติบุคคลที่อยู่ในราชอาณาจักร ไม่ว่าการเก็บ รวบรวม ใช้ หรือเปิดเผยนั้นจะกระทำในหรือนอกราชอาณาจักร ซึ่งจากบทบัญญัติดังกล่าวแสดงให้เห็นชัดเจนว่าการบังคับใช้กฎหมายฉบับนี้อ้างอิง “การตั้งอยู่ของบุคคลหรือนิติบุคคล” ในประเทศไทยเป็นหลัก โดยไม่ได้พิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะอยู่ในหรือนอกราชอาณาจักร

ดังนั้นไม่ว่า (ก) บุคคลธรรมดาสัญชาติใดที่มาอยู่ในราชอาณาจักร หรือ (ข) นิติบุคคลใดที่ได้มีการจดทะเบียนจัดตั้งในราชอาณาจักร และทำการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่น บุคคลและนิติบุคคลดังกล่าวต้องอยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ในทันที

ทั้งนี้ กรณีการประมวลผลข้อมูลส่วนบุคคลโดยบุคคลธรรมดาที่จะอยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ หากเป็นการประมวลผลเพื่อประโยชน์ส่วนตัว ไม่ใช้การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์เชิงการค้าหรือพาณิชย์ บุคคลธรรมดาดังกล่าวจะได้รับการยกเว้นจากการปฏิบัติตามพระราชบัญญัติ (อ้างอิงตามมาตรา 4 (1)) แต่หากไม่ใช้การประมวลผลข้อมูลเพื่อประโยชน์ส่วนตัว แต่เป็นการดำเนินธุรกิจ ยกตัวอย่างเช่น หากบุคคลธรรมดาประกอบธุรกิจและได้ว่าจ้างพนักงานไม่ว่าจะเป็นพนักงานประจำหรือพนักงาน Freelance และมีการใช้ข้อมูลส่วนบุคคลของบุคคลดังกล่าว บุคคลธรรมดาดังกล่าวก็อยู่ภายใต้บังคับต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกันโดยไม่ได้รับการยกเว้น

PDPA ใช้บังคับคุ้มครองข้อมูลส่วนบุคคลของคนที่อยู่ในประเทศไทย : นอกจากการอ้างอิงหลักการตั้งอยู่ของบุคคลหรือนิติบุคคลที่ตั้งอยู่ในราชอาณาจักรแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาตรา 5 กำหนดว่า พระราชบัญญัติฉบับนี้จะมีผลบังคับกับบุคคลหรือนิติบุคคลที่อยู่ในราชอาณาจักรด้วยเช่นกัน แต่การมีผลบังคับใช้นั้นจะจำกัดเฉพาะในกรณีที่กิจกรรมการประมวลผลข้อมูลของบุคคลหรือนิติบุคคลดังกล่าวเป็น (ก) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม หรือ (ข) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

ดังนั้นบทบัญญัติของพระราชบัญญัติฉบับนี้จะมีผลบังคับอ้างอิงตาม “การอยู่ในประเทศของเจ้าของข้อมูลส่วนบุคคล” ด้วยเช่นกัน

แม้ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะดำเนินการโดยบุคคลหรือนิติบุคคลที่อยู่นอกประเทศ แต่หาก Target ของการประมวลผลข้อมูลส่วนบุคคล คือ เจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศไทย การประมวลผลข้อมูลส่วนบุคคลนั้นก็ต้องดำเนินการตาม PDPA เช่นเดียวกัน ยกตัวอย่างเช่น กรณีบริษัท IT Solution ที่ให้บริการระบบการบริหารจัดการทรัพยากรบุคคล (HRM System หรือ HRIS System) แม้จะเป็นบริษัทที่จดทะเบียนอยู่ต่างประเทศ แต่หากมาให้บริการกับองค์กรนายจ้างในไทยเพื่อประมวลผลข้อมูลส่วนบุคคลของพนักงานขององค์กรนายจ้างในประเทศไทย บริษัท IT Solution ดังกล่าวก็ต้องอยู่ภายใต้บังคับของ PDPA เช่นเดียวกัน แม้จะไม่ได้มาจัดตั้งเป็นนิติบุคคลภายใต้กฎหมายประเทศไทยก็ตาม

PDPA ไม่ได้จำกัดการคุ้มครองสิทธิเจ้าของข้อมูลส่วนบุคคลตามสัญชาติของเจ้าของข้อมูลส่วนบุคคล : เจ้าของข้อมูลส่วนบุคคลที่จะได้รับการคุ้มครองสิทธิภายใต้กรอบของ PDPA ไม่ได้ถูกระบุจำกัดไว้ให้มีผลบังคับใช้กับเจ้าของข้อมูลส่วนบุคคลที่มีสัญชาติไทยเท่านั้น ดังจะสังเกตได้ว่าบทบัญญัติกฎหมายไม่ได้ใช้คำว่า “บุคคลสัญชาติไทย” แต่เลือกใช้คำว่า **“ที่อยู่ในประเทศไทย”** ดังนั้นกรณีที่องค์กรที่อยู่ในประเทศไทยประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลไม่ว่าจะเป็นบุคคลสัญชาติใดก็ตาม องค์กรดังกล่าวมีหน้าที่รับประกันในการปฏิบัติหน้าที่ของตนเองให้ครบถ้วนตามที่กำหนดไว้ใน PDPA ทั้งนี้ กรณีที่เจ้าของข้อมูลส่วนบุคคลดังกล่าวอาจได้รับการคุ้มครองสิทธิภายใต้กฎหมายประเทศอื่นด้วย (เช่น GDPR ที่คุ้มครองคนสัญชาติยุโรปไม่ว่าจะอยู่ที่ไหนก็ตาม) แปลว่าองค์กรที่จะประมวลผลข้อมูลส่วนบุคคลของ

เจ้าของข้อมูลส่วนบุคคลดังกล่าวต้องปฏิบัติตามทั้ง PDPA ภายใต้หลักที่ตั้งขององค์กรและกฎหมายของ GDPR โดยอ้างอิงจากสัญญาติของเจ้าของข้อมูลส่วนบุคคลอีกด้วย

สรุปท้ายบท

ประเทศไทยประกาศกำหนดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในปี พ.ศ. 2562 ซึ่งมีผลบังคับในวันที่ 1 มิถุนายน 2565 ด้วยจุดประสงค์หลักคือ

(1) เพื่อให้ประเทศไทยมีกฎหมายที่ให้การคุ้มครองข้อมูลส่วนบุคคลในมาตรฐานเดียวกับประเทศอื่น ๆ โดยเฉพาะสหภาพยุโรป เพื่อให้การส่งต่อและรับข้อมูลที่เป็นข้อมูลส่วนบุคคลจากประเทศต่าง ๆ เหล่านั้นสามารถดำเนินการได้อย่างสมบูรณ์มากขึ้น

(2) เพื่อกำหนดกรอบกฎหมายหลักที่มีหัวข้อคุ้มครองเฉพาะเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งจะเข้ามาช่วยปิดช่องโหว่และแก้ไขปัญหาการบังคับใช้กฎหมายทั่วไป (ทั้งกฎหมายแพ่ง กฎหมายอาญา และกฎหมายเฉพาะ) ที่ยังไม่ตอบโจทย์โดยตรงกับความเสียหายที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล

นอกจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว ปัจจุบันมีการออกกฎหมายลำดับรองโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นคณะกรรมการที่ได้รับการจัดตั้งขึ้นโดยเฉพาะภายใต้พระราชบัญญัติเพื่อทำหน้าที่คุ้มครองและกำกับดูแลการจัดตั้งปฏิบัติของพระราชบัญญัติฉบับนี้โดยตรง ซึ่งผู้ประกอบการต้องให้

ความใส่ใจในการปฏิบัติตามทั้งพระราชบัญญัติและกฎหมายลำดับรอง เพื่อป้องกันผลกระทบและความเสี่ยงที่อาจเกิดจากการดำเนินการประมวลผลข้อมูลส่วนบุคคลอย่างไม่ถูกต้อง ซึ่งอาจรวมถึงการได้รับคำสั่งทางปกครองหรือการลงโทษปกครองโดยคณะกรรมการผู้เชี่ยวชาญ

แม้จะมีบางการประมวลผลข้อมูลส่วนบุคคล (Data Flow) ที่ดำเนินการโดยหน่วยงานรัฐและเอกชน ในบางส่วนที่ได้รับการยกเว้นจากการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางมาตรา อ้างอิงตามมาตรา 4 ของพระราชบัญญัติ แต่หน้าที่หลักที่หน่วยงานต่าง ๆ ยังต้องดำเนินการตามโดยไม่ได้รับยกเว้น ได้แก่ หน้าที่ในการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลที่ตนเก็บรวบรวมทั้งหมด ไม่ว่าจะเป็นการได้มาหรือการประมวลผลข้อมูลในกระบวนการที่ได้รับการยกเว้นจากการปฏิบัติตามหน้าที่ตามพระราชบัญญัติหรือไม่ และนอกเหนือจากกระบวนการ (Data Flow) ที่ได้รับการยกเว้นแล้ว หน่วยงานดังกล่าวยังคงมีหน้าที่ต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในการดำเนินการประมวลผลข้อมูลส่วนบุคคลในขั้นตอนอื่น ๆ นั้นอย่างครบถ้วนโดยไม่ได้รับข้อยกเว้น และหนึ่งในกระบวนการที่อยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลทั้งหมดในทุกขั้นตอน ได้แก่ กระบวนการขั้นตอนการประมวลผลข้อมูลส่วนบุคคลของพนักงาน บุคลากรภายในของหน่วยงานดังกล่าว

ภายใต้กรอบของมาตรา 5 บุคคลหรือนิติบุคคลที่จะอยู่ภายใต้บังคับของ PDPA แบ่งออกเป็น 2 กลุ่ม คือ

(1) บุคคลหรือนิติบุคคลที่อยู่ในประเทศไทย (อาศัยอยู่หรือจดทะเบียนจัดตั้งภายใต้กฎหมายประเทศไทย) ไม่ว่าบุคคลหรือ

นิติบุคคลดังกล่าวจะดำเนินการประมวลผลข้อมูลส่วนบุคคลนั้น
ในหรือนอกราชอาณาจักร และ

(2) บุคคลหรือนิติบุคคลที่แม้อยู่นอกประเทศไทย แต่ดำเนินการ
ประมวลผลข้อมูลส่วนบุคคลเจ้าของข้อมูลส่วนบุคคลที่อยู่ใน
ในประเทศไทย เพื่อการนำเสนอสินค้าหรือบริการหรือการเฝ้าติดตาม
พฤติกรรมก็ตาม

ทั้งนี้ PDPA มีผลคุ้มครองเจ้าของข้อมูลบุคคลที่อยู่ในประเทศไทย
ไม่ว่าเจ้าของข้อมูลส่วนบุคคลนั้นจะเป็นบุคคลสัญชาติไทยหรือไม่ก็ตาม



บทที่ 02

นิยามศัพท์ที่สำคัญ

ภายใต้พระราชบัญญัติ

คุ้มครองข้อมูลส่วนบุคคล

เมื่อเข้าใจถึงภาพรวมจุดประสงค์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว สิ่งที่ต้องทำความเข้าใจถัดมาคือ นิยามบางคำศัพท์ที่สำคัญภายใต้กรอบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เข้าใจลึกซึ้งถึงกรอบการบังคับใช้ของ PDPA ลงไปในรายละเอียดเพิ่มเติมว่า “การประมวลผลข้อมูลในลักษณะรูปแบบใดบ้างที่อยู่ภายใต้บังคับของ PDPA” และองค์กรที่ใช้ข้อมูลส่วนบุคคลดังกล่าว ถูกจัดให้อยู่ในฐานะและหน้าที่ความรับผิดชอบใดภายใต้กรอบของ PDPA

บทที่ 2 นี้จะอธิบายและยกตัวอย่างการตีความนิยามศัพท์ที่สำคัญ ได้แก่ “ข้อมูลส่วนบุคคล” “การประมวลผลข้อมูลส่วนบุคคล” “ผู้ควบคุมข้อมูลส่วนบุคคล” “ผู้ประมวลผลข้อมูลส่วนบุคคล” และ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล”

2.1 ข้อมูลส่วนบุคคล

PDPA มีผลคุ้มครองเฉพาะ “ข้อมูลส่วนบุคคล” ดังนั้นนิยามศัพท์สำคัญที่ต้องทำความเข้าใจคือ ข้อมูลใดบ้างที่เข้านิยามข้อมูลส่วนบุคคล

นอกจากนี้ PDPA ยังได้กำหนดระดับความอ่อนไหวของข้อมูลส่วนบุคคลบางประเภทไว้ พร้อมกับกำหนดความคาดหวังที่เข้มงวดมากขึ้นในการคุ้มครองข้อมูลส่วนบุคคลอ่อนไหวประเภทดังกล่าวไว้ด้วย ผู้ใช้ข้อมูลส่วนบุคคลจึงควรทำความเข้าใจนิยามและขอบเขตข้อมูลส่วนบุคคลที่อาจมีความอ่อนไหวดังกล่าวเพิ่มเติมเพื่อการแยกประเภทข้อมูลและการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลที่อ่อนไหวดังกล่าวได้อย่างเหมาะสมตามกรอบที่ PDPA ต้องการอีกด้วย

Q1 : ภายใต้ PDPA ข้อมูลที่จะถือเป็นข้อมูลส่วนบุคคล ต้องมีลักษณะอย่างไร ?

PDPA มีผลคุ้มครองเฉพาะ “ข้อมูลส่วนบุคคล”

ดังนั้นนิยามศัพท์ที่สำคัญที่ต้องทำความเข้าใจคือ ข้อมูลใดบ้างที่เข้านิยามข้อมูลส่วนบุคคล ภายใต้กรอบของกฎหมาย มาตรา 6 ของ PDPA ระบุว่า “**ข้อมูลส่วนบุคคล** หมายถึง **ข้อมูลเกี่ยวกับบุคคล** ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

จากนิยามภายใต้มาตราดังกล่าว องค์ประกอบของ “ข้อมูลส่วนบุคคล” มีดังนี้

1. ข้อมูลที่จะถือเป็นข้อมูลส่วนบุคคลต้องเป็นข้อมูลของ**บุคคลธรรมดาที่มีชีวิตอยู่** ดังนั้นข้อมูลที่เกี่ยวข้องกับองค์กรหรือนิติบุคคลทั้งหมด ไม่ถือเป็นข้อมูลส่วนบุคคล เช่น หนังสือรับรองบริษัท ใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.20) หรือเอกสารงบการเงินของบริษัทต่าง ๆ ไม่ถือเป็นข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม เอกสารของบริษัทบางส่วนอาจมีข้อมูลของคนธรรมดาอยู่ เช่น ชื่อนามสกุลของกรรมการหรือผู้ถือหุ้น เป็นต้น ซึ่งจำเป็นต้องประเมินและตรวจสอบแยกส่วนกันว่าส่วนใดเป็นข้อมูลส่วนบุคคลที่ต้องให้ความสนใจพิจารณาตาม PDPA และส่วนใดเป็นข้อมูลของบริษัทโดยแท้

นอกจากประเด็นที่ว่าข้อมูลส่วนบุคคลนั้นต้องเป็นข้อมูลของบุคคลธรรมดา ไม่ใช่นิติบุคคลแล้ว PDPA กำหนดชัดเจนว่าข้อมูลที่จะเป็นข้อมูลส่วนบุคคลต้องเป็นข้อมูลของบุคคลที่ยังมีชีวิตอยู่

ดังนั้นเมื่อบุคคลดังกล่าวเสียชีวิต ข้อมูลที่เกี่ยวข้องใช้เพื่อการระบุตัวตนบุคคลดังกล่าวจะไม่ถือเป็นข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองภายใต้ PDPA อีกต่อไป การใช้ข้อมูลของผู้วายชนม์ดังกล่าวไม่ถือว่าอยู่ภายใต้บังคับของ PDPA แต่อย่างไรก็ตาม ในการใช้ข้อมูลดังกล่าวอาจอยู่ภายใต้บังคับการคุ้มครองภายใต้กฎหมายทั่วไปอื่น ซึ่งต้องได้รับการพิจารณา เช่น กฎหมายอาญา มาตรา 327 (การหมิ่นประมาทผู้ตาย) เป็นต้น

2. ข้อมูลที่จะถือเป็นข้อมูลส่วนบุคคลต้องสามารถระบุตัวบุคคลธรรมดาคนหนึ่งคนได้ ไม่ว่าด้วยการใช้ข้อมูลนั้นเดียว ๆ หรือการใช้ข้อมูลนั้นประกอบกับข้อมูลอื่น ๆ ทั้งนี้ การระบุตัวตนได้หมายถึง หากได้ข้อมูลนั้นมาแล้ว ผู้ได้รับข้อมูลสามารถใช้ข้อมูลนั้นไปชี้หรือติดต่อบุคคลธรรมดาคนหนึ่งได้ แยกคนคนนั้นออกจากกลุ่มคนอื่น ๆ ได้ทั้งนี้ PDPA มุ่งเน้นที่การระบุตัวตนไม่ใช่การรู้จักตัวตน ดังนั้นหากข้อมูลนั้นสามารถใช้เพื่อการติดต่อประสานงานหรือชี้ไปยังบุคคลใดบุคคลหนึ่งได้ แม้ไม่ทราบว่าบุคคล ๆ นั้นชื่ออะไรหรือเป็นใคร ก็ถือว่าข้อมูลนั้นเป็นข้อมูลส่วนบุคคลในทันที

ข้อมูลส่วนบุคคลทางตรง นอกจากข้อมูลชื่อ-นามสกุล บัตรประจำตัวประชาชน ที่แน่นอนทุกคนทราบว่าเป็นข้อมูลส่วนบุคคลแล้ว ยังรวมถึงข้อมูลตัวอย่างเช่น

(ก) ข้อมูลภาพถ่ายที่ติดใบหน้าบุคคล เนื่องจากเมื่อได้ข้อมูลดังกล่าวมาผู้เก็บรวบรวมข้อมูลนั้นมาสามารถเอารูปนั้นไปชี้ตัวบุคคลที่เป็นเจ้าของใบหน้าในรูปได้ ข้อมูลภาพถ่ายนั้นถือเป็นข้อมูลส่วนบุคคลทันที แม้ว่าผู้เก็บข้อมูลนั้นจะไม่ทราบชื่อนามสกุลหรือไม่ทราบว่าบุคคลในภาพเป็นใครก็ตาม

(ข) ข้อมูลการติดต่อ เช่น e-Mail ที่แม้จะไม่ได้เป็นอีเมลที่ระบุชื่อ เช่น hello1234@gmail.com หรือเป็น Social Media Account ที่ไม่ได้ใช้ชื่อจริง แต่เมื่อผู้ได้รับข้อมูลใช้อีเมลหรือ Social Media Account นั้นจะสามารถติดต่อไปยังบุคคลธรรมดาคนคนหนึ่งได้ในทันที ข้อมูลดังกล่าวจึงเข้านิยามการเป็น “ข้อมูลส่วนบุคคล” ภายใต้กรอบของ PDPA ทันทีเช่นกัน

(ค) ข้อมูลคำอธิบายที่ไม่ได้มีข้อมูลที่เหมือนจะระบุตัวตนทางตรง แต่เมื่อพิจารณาประกอบกับบริบทโดยรวมแล้ว สามารถระบุตัวบุคคลได้ เช่น ผู้หญิงใส่แว่นที่ถือไม้ค้ำยันอยู่หน้าห้องบรรยาย ณ ตอนนี้ เมื่อพิจารณาเนื้อหาของข้อมูลแล้ว ไม่มีข้อมูลใดที่เหมือนจะระบุตัวบุคคลได้เลย แต่เนื่องจากในห้องบรรยาย ณ เวลานั้น มีผู้หญิงใส่แว่นอยู่คนเดียว กรณีนี้ข้อมูลคำอธิบายดังกล่าวก็ถือเป็นข้อมูลส่วนบุคคลเช่นกัน แต่จะเป็นข้อมูลส่วนบุคคลเฉพาะบุคคลที่อยู่ในห้องบรรยาย ณ เวลานั้นเท่านั้น

ข้อมูลส่วนบุคคลทางอ้อม นอกจากข้อมูลที่เป็นข้อมูลส่วนบุคคลโดยตรงตามตัวอย่างข้างต้นแล้ว นิยามของข้อมูลส่วนบุคคลภายใต้ PDPA ยังรวมถึงข้อมูลที่เมื่อนำมาประกอบกันกับข้อมูลอื่น ๆ แล้วสามารถใช้เพื่อการระบุตัวบุคคลธรรมดาคนหนึ่งได้ด้วยเช่นกัน ตัวอย่างเช่น

(ก) ข้อมูลที่อยู่บ้านหากเป็นข้อมูลที่อยู่เดียว ๆ อาจไม่ถือเป็นข้อมูลส่วนบุคคล เนื่องจากที่อยู่บ้านหลังหนึ่งอาจมีคนอาศัยอยู่มากกว่า 1 คน ดังนั้นเพียงข้อมูลที่อยู่จึงไม่ได้มีลักษณะเป็นข้อมูลส่วนบุคคล แต่หากเป็นที่อยู่ที่ได้มาพร้อมกับชื่อ-นามสกุลเพื่อการจัดส่งสินค้า ซึ่งจะมีการระบุชื่อผู้รับคนใดคนหนึ่งมาด้วย เมื่อที่อยู่นั้นสามารถอ่าน