

แนวปฏิบัติของภาคธุรกิจประกันวินาศภัย
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
(ฉบับปรับปรุงแก้ไข ครั้งที่ 1)

The Personal Data Protection Act B.E. 2562 Guideline
for the Non-Life Insurance Industry
(Amendment No. 1)



ภายใต้ความร่วมมือ



แนวปฏิบัติของภาคธุรกิจประกันวินาศภัยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พิมพ์ครั้งที่	1
จำนวนหน้า	351 หน้า
ผู้จัดทำ	สมาคมประกันวินาศภัยไทย 25 ซอยสุขุมวิท 64/1 ถนนสุขุมวิท แขวงพระโขนงใต้ เขตพระโขนง กรุงเทพฯ 10260
ภายใต้ความร่วมมือ	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.)
ผู้เขียน	นางสาวอริษฐา จิตรานุเคราะห์ นายธรรม์ บุรพวัฒน์ นางสาวธรรมพรพรช ชาญพานิช บริษัท ทิลลิเกีแอนด์กิบินส์ อินเตอร์เนชั่นแนล จำกัด
ผู้เรียบเรียง	คณะกรรมการกฎหมายและกฎระเบียบ สมาคมประกันวินาศภัยไทย
วันที่เผยแพร่	-
วันที่ปรับปรุงแก้ไข	ครั้งที่ 1 วันที่ 31 มีนาคม 2566

สมาคมประกันวินาศภัยไทยได้จัดทำแนวปฏิบัติฉบับนี้ขึ้นเพื่อเป็นแนวทางในการดำเนินการต่าง ๆ ที่เกี่ยวข้อง กับข้อมูลส่วนบุคคลสำหรับภาคธุรกิจประกันวินาศภัยเท่านั้น การเผยแพร่ แก้ไข เปลี่ยนแปลง หรือทำซ้ำ จะต้องได้รับความยินยอมจากสมาคมประกันวินาศภัยไทย

คำนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นกฎหมายหลักที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของไทยที่จะมีผลบังคับใช้ในเวลาอันใกล้ ส่งผลให้ทุกภาคส่วนต้องมีการเตรียมความพร้อมในการรับมือเพื่อให้สามารถปฏิบัติตามกฎหมายดังกล่าวได้ตามกำหนดเวลา

ธุรกิจประกันวินาศภัยถือเป็นธุรกิจที่ให้บริการทางการเงินซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลตลอดห่วงโซ่อุปทาน ตั้งแต่การพิจารณารับประกันภัย การบริหารจัดการค่าสินไหมทดแทน ไปจนถึงการประกันภัยต่อการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จึงต้องกระทำด้วยความระมัดระวังและรอบคอบเพื่อป้องกันไม่ให้เกิดการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล และในขณะเดียวกัน ก็ต้องมีความสมเหตุสมผลในการดำเนินการเพื่อไม่ให้เป็นการอุปสรรคในการประกอบธุรกิจ

สมาคมประกันวินาศภัยไทยได้เล็งเห็นถึงความสำคัญในการเตรียมความพร้อมเพื่อให้บริษัทประกันวินาศภัยในประเทศไทยสามารถปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างถูกต้อง ครบถ้วน มีประสิทธิภาพและประสิทธิผล สมาคมประกันวินาศภัยไทยจึงได้จัดทำแนวปฏิบัติฉบับนี้ขึ้นเพื่อเป็นแนวทางในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของภาคธุรกิจประกันวินาศภัยไทย แต่เนื่องจากกฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังอยู่ในระหว่างการจัดทำในเวลานี้ เมื่อมีการประกาศใช้กฎหมายลำดับรองดังกล่าวแล้ว แนวปฏิบัตินี้อาจต้องได้รับการทบทวนและปรับปรุงเพื่อให้เหมาะสมและสอดคล้องกับกฎหมายที่จะมีเพิ่มเติมในอนาคตต่อไป

สมาคมประกันวินาศภัยไทยหวังเป็นอย่างยิ่งว่า แนวปฏิบัติฉบับนี้จะเป็นประโยชน์ต่อภาคธุรกิจประกันวินาศภัยไทยรวมถึงทุกภาคส่วนที่เกี่ยวข้อง และช่วยให้ธุรกิจประกันวินาศภัยสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างสมบูรณ์ และทำหน้าที่เป็นผู้บริหารความเสี่ยงมีอาชีพให้กับภาครัฐและเอกชนได้อย่างยั่งยืน

(นายอานนท์ วังวสุ)

นายกสมาคมประกันวินาศภัยไทย

สารบัญ

คำจำกัดความ	8
บทที่ 1 ขอบเขตการใช้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	9
1.1 ความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย	9
1.2 ขอบเขตการใช้บังคับของกฎหมาย.....	13
1.3 การจัดการข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีผลบังคับใช้	24
1.4 การปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอื่น ..	29
บทที่ 2 หลักการพื้นฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.....	33
2.1 ความชอบด้วยกฎหมาย และความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคล	33
2.2 ข้อจำกัดด้านวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล	35
2.3 ความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล	37
2.4 ความถูกต้อง สมบูรณ์ และเป็นปัจจุบันของข้อมูลส่วนบุคคล	37
2.5 ความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคล	38
2.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล	38
2.7 หลักความรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล	39
บทที่ 3 ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล	40
3.1 ผู้ควบคุมข้อมูลส่วนบุคคล	40
3.2 ผู้ประมวลผลข้อมูลส่วนบุคคล	50
3.3 ตัวอย่างการพิจารณาผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล.....	52
บทที่ 4 แนวทางการแยกประเภทข้อมูลส่วนบุคคล	55
4.1 ขอบเขตและประเภทข้อมูลส่วนบุคคล.....	55
4.2 แนวทางการแยกประเภทข้อมูลส่วนบุคคล	58
บทที่ 5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	62

5.1 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป	64
5.2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว	91
5.3 การเปลี่ยนวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	106
5.4 แนวทางการกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล	107
5.5 แนวทางการส่งหรือโอนข้อมูลส่วนบุคคลในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันในประเทศ	110
5.6 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น	111
5.7 แนวทางการบันทึกการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ. คู้มครองข้อมูลส่วนบุคคล	116
5.8 แนวทางการแลกเปลี่ยนข้อมูลส่วนบุคคลที่กระทำความผิดอาญาเกี่ยวกับการประกันวินาศภัย	118
บทที่ 6 การโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ	119
6.1 หลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ.....	119
6.2 ข้อยกเว้นของเงื่อนไขในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ.....	119
6.3 ข้อยกเว้นสำหรับการโอนข้อมูลส่วนบุคคลไปยังบริษัทในเครือ หรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน.....	120
6.4 ข้อยกเว้นอื่น.....	123
บทที่ 7 แนวทางการปฏิบัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล	125
7.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล.....	126
7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล.....	143
7.3 แนวทางปฏิบัติเมื่อมีการร้องขอให้เปิดเผยข้อมูลส่วนบุคคลจากหน่วยงานรัฐ.....	149
บทที่ 8 แนวทางการปฏิบัติกรณีเกิดละเมิดข้อมูลส่วนบุคคล	154
8.1 หน้าที่และความรับผิดชอบของบริษัท กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล.....	154
8.2 กรณีศึกษาเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล	170
บทที่ 9 หน้าที่ที่คู้มครองข้อมูลส่วนบุคคล	174
9.1 หน้าที่ในการตั้งเจ้าหน้าที่คู้มครองข้อมูลส่วนบุคคล	174
9.2 คุณสมบัติของเจ้าหน้าที่คู้มครองข้อมูลส่วนบุคคล	175
9.3 เงื่อนไขเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คู้มครองข้อมูลส่วนบุคคล	176
9.4 หน้าที่ของเจ้าหน้าที่คู้มครองข้อมูลส่วนบุคคล	178

9.5	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล.....	179
9.6	การกระทำความผิดที่อาจเกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	179
บทที่ 10	ความรับผิดและบทกำหนดโทษตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	181
10.1	สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล	181
10.2	ความรับผิดและการกระทำความผิดของผู้ประมวลผลข้อมูลส่วนบุคคล.....	192
10.3	รายละเอียดความรับผิดทางแพ่ง	197
10.4	โทษทางอาญาของกรรมการหรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล	199
10.5	โทษทางปกครอง.....	200
บทที่ 11	ตัวอย่างร่างข้อความในเอกสารทางกฎหมายที่สำคัญตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	202
11.1	ตัวอย่างร่างข้อความแจ้งและการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลสำหรับลูกค้าและผู้มุ่งหวัง	202
11.2	ตัวอย่างร่างข้อความแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคลสำหรับคู่ค้า (รวมทั้งนายหน้าประกันวินาศภัย)	215
11.3	ตัวอย่างร่างข้อความแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลสำหรับพนักงาน.....	225
11.4	ตัวอย่างแบบความยินยอมสำหรับการดำเนินกิจกรรมทางการตลาด	236
11.5	ตัวอย่างร่างข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคล	238
11.6	ตัวอย่างร่างคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	250
11.7	ตัวอย่างร่างการแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคล	256
11.8	ตัวอย่างการแจ้งช่องทางการถอนความยินยอมตามมาตรา 95.....	258
11.9	ตัวอย่างแบบการบันทึกการประมวลผลข้อมูลส่วนบุคคล	260
11.10	ตัวอย่างคำรับรองสำหรับผู้ถือกรรมธรรม์ประกันภัย หนังสือรับรองการได้รับความยินยอมจากสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ.....	267
บทที่ 12	เอกสารแนบ	270
12.1	แนวทางการปฏิบัติด้านทรัพยากรบุคคล	270
12.2	แนวทางการดำเนินการในการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ข้อมูลส่วนบุคคล	278
12.3	ตัวอย่างข้อมูลส่วนบุคคล และฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	282

12.4 แนวปฏิบัติเกี่ยวกับ Three Lines of Defense สำหรับการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	286
12.5 แนวทางปฏิบัติเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	289
12.6 แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในของบริษัท	310
12.7 สรุปเงื่อนไขการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	313
12.8 การไหลเวียนของข้อมูลส่วนบุคคล (Data Flow) สำหรับบริษัท	320

คำจำกัดความ

กระทรวงดิจิทัล	= กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
คณะกรรมการ	= คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
คปภ.	= คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
บริษัท	= บริษัทประกันวินาศภัย
ป.พ.พ.	= ประมวลกฎหมายแพ่งและพาณิชย์
ป.วิ.พ.	= ประมวลกฎหมายวิธีพิจารณาความแพ่ง
ป.วิ.อ.	= ประมวลกฎหมายวิธีพิจารณาความอาญา
ป.อ.	= ประมวลกฎหมายอาญา
ปปง.	= สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
ประมวลผล	= เก็บรวบรวม ใช้ หรือเปิดเผย
พ.ร.บ.	= พระราชบัญญัติ
พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน	= พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	= พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
พนักงานเจ้าหน้าที่	= พนักงานเจ้าหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
รัฐมนตรี	= รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
เลขาธิการ	= เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
สมาคม	= สมาคมประกันวินาศภัยไทย
สำนักงาน	= สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
สำนักงาน คปภ.	= สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
UKDPA	= United Kingdom Data Protection Act 2018
SGPDPA	= Singapore Personal Data Protection Act 2012
GDPR	= European Union General Data Protection Regulation

บทที่ 1 ขอบเขตการใช้บังคับ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.1 ความเป็นมาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

เดิมก่อนที่จะมีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ภาครัฐได้มีความพยายามที่จะจัดให้มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเป็นระยะเวลานานกว่า 10 ปี โดยเล็งเห็นถึงความก้าวหน้าทางเทคโนโลยี การคุ้มครองความเป็นส่วนตัว และแนวโน้มการละเมิดสิทธิในข้อมูลส่วนบุคคล และสิทธิความเป็นส่วนตัวที่เพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไปเปิดเผยโดยมิชอบหรือเปิดเผยโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลเพื่อแสวงหาประโยชน์ต่าง ๆ จึงมีการศึกษาและร่างกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น

ในปี พ.ศ. 2561 สหภาพยุโรป (European Union) ได้ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ que เรียกกันว่า General Data Protection Regulation (“GDPR”) ซึ่งนอกจากมีผลบังคับใช้ภายในประเทศสมาชิกของสหภาพยุโรปแล้ว ยังกำหนดให้บุคคลหรือองค์กรที่อยู่ภายนอกสหภาพยุโรป (ซึ่งอาจรวมถึงผู้ประกอบการในประเทศไทยในบางกรณี) ต้องปฏิบัติตาม GDPR รวมถึงมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอด้วย หากบุคคลหรือองค์กรเหล่านั้นประกอบธุรกิจโดยมีความเกี่ยวข้องกับบุคคลในสหภาพยุโรป

การประกาศใช้ GDPR นั้น ได้ก่อให้เกิดกระแสในระดับนานาชาติ รวมถึงการตอบรับจากรัฐบาลไทยถึงความสำคัญของการจัดให้มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป และทำให้เกิดการผลักดันยกร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลขึ้น และพัฒนาจนสามารถประกาศใช้เป็นกฎหมายได้ในวันที่ 27 พฤษภาคม 2562 โดยหลักการรวมถึงบทบัญญัติส่วนใหญ่ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลนั้น อ้างอิงมาจากหลักเกณฑ์ของ GDPR เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของไทยเป็นไปตามมาตรฐานสากล

หลังจากที่มีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเมื่อวันที่ 27 พฤษภาคม 2562 ภาคธุรกิจได้มีการตื่นตัวในการเตรียมความพร้อมเพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก โดยเฉพาะภาคธุรกิจที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นจำนวนมาก เช่น ภาคธุรกิจการเงิน การธนาคาร ภาคธุรกิจประกันภัย รวมถึงภาคธุรกิจที่เกี่ยวข้องกับสุขภาพ เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลนี้ได้กำหนดระยะเวลาให้ผู้ประกอบธุรกิจสามารถดำเนินการเพื่อปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้จนถึงวันที่ 31 พฤษภาคม 2565 ก่อนที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจะมีผลใช้บังคับทั้งฉบับในวันที่ 1 มิถุนายน 2565

อย่างไรก็ตาม ก่อนที่ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคลนี้จะประกาศใช้บังคับในราชกิจจานุเบกษา ประเทศไทยได้มีกฎหมายที่เกี่ยวกับการคຸ່ມครองข้อมูลส่วนบุคคลอยู่ก่อนแล้ว เพียงแต่เป็นในลักษณะของกฎหมายเฉพาะกลุ่มธุรกิจ เช่น ในภาคธุรกิจสถาบันการเงิน ได้มีประกาศธนาคารแห่งประเทศไทยในเรื่อง Market Conduct¹ ที่มีการกำหนดในเรื่องของการคຸ່ມครองข้อมูลส่วนบุคคลของลูกค้าธนาคารไว้ ภาคธุรกิจโทรคมนาคม มีประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคຸ່ມครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม² ภาคธุรกิจสาธารณสุข มีระเบียบกระทรวงสาธารณสุข เรื่อง การคຸ່ມครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561³ เป็นต้น

ในส่วนของสำนักงาน คปภ. ก็ได้มีการออกประกาศสำนักงาน เรื่องแนวปฏิบัติในการคຸ່ມครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 เพื่อกำหนดกรอบการกำกับเกี่ยวกับการคຸ່ມครองข้อมูลส่วนบุคคลสำหรับภาคธุรกิจประกันภัย เนื่องด้วยลักษณะเฉพาะของธุรกิจประกันภัยที่ต้องมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจำนวนมาก สำนักงาน คปภ. จึงเห็นสมควรให้จัดให้มีประกาศดังกล่าวเพื่อให้เป็นแนวทางของภาคธุรกิจ ซึ่งเป็นแนวทางที่สอดคล้องกับประเทศอื่น ๆ เช่น ประเทศสหราชอาณาจักรได้แก้ไข Data Protection Act 2018 (UKDPA) โดยการเพิ่มฐานการประมวลผลข้อมูลส่วนบุคคลฐาน “Insurance Purpose”⁴ สำหรับข้อมูลส่วนบุคคลประเภทพิเศษ เป็นต้น (ทั้งนี้ ณ ปัจจุบันประเทศสหราชอาณาจักรอยู่ในช่วงดำเนินการออกจากกลุ่มสหภาพยุโรป ดังนั้น จึงอยู่ระหว่างการดำเนินงานแก้ไขกฎหมายที่เกี่ยวข้องกับการคຸ່ມครองข้อมูลส่วนบุคคล)

โครงสร้างของ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล

โครงสร้างของ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคลเริ่มต้นด้วยส่วนที่เป็นบทบัญญัติทั่วไปเหมือนกับ พ.ร.บ. อื่น ๆ และมีเนื้อหาในส่วนอื่น ๆ แบ่งออกเป็น 7 หมวด ดังนี้

บทบัญญัติทั่วไป (มาตรา 1 – มาตรา 7)

บทบัญญัติทั่วไปกำหนดเกี่ยวกับเรื่องผลบังคับใช้ของกฎหมาย และบทนิยามตาม พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล

¹ ประกาศธนาคารแห่งประเทศไทย ที่ สกส. 1/2561 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct) เอกสารแนบท้าย 1

² ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคຸ່ມครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม

³ ระเบียบกระทรวงสาธารณสุข เรื่อง การคຸ່ມครองและจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. 2561 หมวด 2

⁴ United Kingdom Data Protection Act 2018, Schedule 1, Part 2

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 8 – มาตรา 18)

บทบัญญัติส่วนนี้จะมีการระบุกฎเกณฑ์ คุณสมบัติ รวมถึงอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (“คณะกรรมการ”)

หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 19 – มาตรา 29)

บทบัญญัติส่วนนี้แบ่งเนื้อหาออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 บททั่วไป (มาตรา 19 - มาตรา 21) บทบัญญัติในส่วนนี้กำหนดเกี่ยวกับหลักของการขอความยินยอมในกรณีทั่วไป การขอความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ และหลักในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์

ส่วนที่ 2 การเก็บรวบรวมข้อมูล (มาตรา 22 – มาตรา 26) บทบัญญัติในส่วนนี้กล่าวถึงฐานอันชอบธรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลประเภทที่ระบุไว้เป็นพิเศษ หรือเรียกว่า “ข้อมูลที่มีความอ่อนไหว” (Sensitive Personal Data) รวมถึงหลักเกณฑ์เกี่ยวกับการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

ส่วนที่ 3 การใช้และการเปิดเผยข้อมูลส่วนบุคคล (มาตรา 27 – มาตรา 29) บทบัญญัติในส่วนนี้กำหนดหลักเกณฑ์ในเรื่องการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 30 – 42)

บทบัญญัติส่วนนี้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล การเรียกร้องตามสิทธิ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงคุณสมบัติและหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43 – มาตรา 70)

บทบัญญัติส่วนนี้กำหนดให้มีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งกำหนดอำนาจหน้าที่ของสำนักงาน รวมถึงคุณสมบัติของพนักงานเจ้าหน้าที่ของสำนักงาน

หมวด 5 การร้องเรียน (มาตรา 71 – มาตรา 76)

บทบัญญัติส่วนนี้กำหนดขั้นตอนการร้องเรียนเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ต่อสำนักงาน รวมถึงกำหนดขั้นตอนในการพิจารณาเรื่องร้องเรียนดังกล่าว

หมวด 6 ความรับผิดชอบทางแพ่ง (มาตรา 77 – มาตรา 78)

บทบัญญัติส่วนนี้กำหนดหลักของความรับผิดชอบทางแพ่งเกี่ยวกับการไม่ปฏิบัติตาม พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล รวมถึงการกำหนดให้ศาลมีอำนาจพิจารณาให้บุคคลจ่ายค่าสินไหมทดแทนเชิงลงโทษได้

หมวด 7 บทกำหนดโทษ

บทบัญญัติส่วนนี้กำหนดโทษ ซึ่งแบ่งออกเป็น 2 ส่วน คือ

ส่วนที่ 1 โทษอาญา (มาตรา 79 – มาตรา 81)

ส่วนที่ 2 โทษทางปกครอง (มาตรา 82 – มาตรา 90)

บทเฉพาะกาล (มาตรา 91 – มาตรา 96)

บทบัญญัติส่วนนี้กำหนดการจัดการในการเตรียมการเพื่อปฏิบัติตามกฎหมาย ผู้ดำรงตำแหน่งต่าง ๆ ระหว่างที่ยังไม่มีการแต่งตั้งคณะกรรมการคຸ້ມครองข้อมูลส่วนบุคคล รวมถึงการจัดการเกี่ยวกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมมาก่อนที่ พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคลมีผลใช้บังคับ

บทบัญญัติในหมวดต่าง ๆ ของ พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล เริ่มมีผลใช้บังคับที่ต่างกัน ดังนี้

บทบัญญัติมีผลบังคับใช้ในวันถัดจากวันที่ประกาศลงราชกิจจานุเบกษา (วันที่ 28 พฤษภาคม 2562)

1. บทบัญญัติทั่วไป (มาตรา 1 ถึง มาตรา 7)
2. บทบัญญัติเกี่ยวกับคณะกรรมการคຸ້ມครองข้อมูลส่วนบุคคล (หมวดที่ 1)
3. บทบัญญัติเกี่ยวกับสำนักงานคຸ້ມครองข้อมูลส่วนบุคคล (หมวดที่ 4)
4. บทเฉพาะกาล (มาตรา 91 ถึง มาตรา 94)

บทบัญญัติ ซึ่งจะมีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 มีดังนี้

1. บทบัญญัติเกี่ยวกับการคຸ້ມครองข้อมูลส่วนบุคคล (หมวดที่ 2)
2. บทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล (หมวดที่ 3)
3. บทบัญญัติเกี่ยวกับการร้องเรียนการละเมิดกฎหมาย (หมวดที่ 5)
4. บทบัญญัติเกี่ยวกับความรับผิดตามกฎหมาย (หมวดที่ 6 และหมวดที่ 7)

5. บทเฉพาะกาล (มาตรา 95 และมาตรา 96)

1.2 ขอบเขตการใช้บังคับของกฎหมาย

ขอบเขตการใช้บังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล สามารถพิจารณาได้ 2 มิติ กล่าวคือ 1) ขอบเขตการใช้บังคับด้านเนื้อหา และ 2) ขอบเขตการใช้บังคับใช้ตามหลักดินแดน ซึ่งมีรายละเอียดดังต่อไปนี้

1.2.1 ขอบเขตการใช้บังคับด้านเนื้อหา

หมายถึง ขอบเขตการใช้บังคับใช้ตามหลักเกณฑ์ที่กำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

บุคคลที่ได้รับความคุ้มครองตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ตามมาตรา 6 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้ให้คำนิยามที่สามารถแสดงถึงขอบเขตการใช้บังคับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลได้ ดังนี้

“ข้อมูลส่วนบุคคล” (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“บุคคล” (Person) หมายความว่า บุคคลธรรมดา (Natural Person)

คำนิยามข้างต้น แสดงให้เห็นว่า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ใช้บังคับกับข้อมูลเกี่ยวกับ **บุคคลธรรมดา**ซึ่งทำให้สามารถระบุตัวบุคคลธรรมดาคนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม **และไม่ใช้บังคับกับข้อมูลที่สามารถระบุไปยังตัวนิติบุคคลได้**

นอกจากนี้แล้ว คำนิยามของคำว่า “ข้อมูลส่วนบุคคล” ยังกำหนดกรณีที่เป็นข้อมูลของบุคคลธรรมดา แต่ไม่ถือว่าเป็นข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล นี้ด้วย กล่าวคือ ข้อมูลของผู้ที่ถึงแก่ความตายแล้ว จะไม่ถือว่าเป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลนี้ ดังนั้น การประมวลผลข้อมูลส่วนบุคคลของผู้ที่ถึงแก่ความตายจึงสามารถกระทำได้โดยไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

จากนิยามข้างต้นสามารถสรุปได้ว่า **“ข้อมูลส่วนบุคคล”** ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล คือข้อมูลที่มีลักษณะหรือองค์ประกอบ ดังนี้

- 1) เป็นข้อมูลของบุคคลธรรมดา (Natural Person)
- 2) เจ้าของข้อมูลส่วนบุคคลยังไม่ถึงแก่ความตาย
- 3) ข้อมูลนั้นสามารถระบุตัวบุคคลได้ไม่ว่าทางตรง หรือทางอ้อม

ดังนั้น ข้อมูลใดที่ไม่มีลักษณะ 3 ประการดังที่ระบุข้างต้น ข้อมูลนั้นไม่จัดเป็น “ข้อมูลส่วนบุคคล” ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล การประมวลผลข้อมูลดังกล่าวจึงไม่ต้องดำเนินการตามหลักเกณฑ์และเงื่อนไขที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างข้อมูลส่วนบุคคลในธุรกิจประกันวินาศภัย

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	ประเภทข้อมูลส่วนบุคคล (Personal Data)
ผู้มุ่งหวัง	1. ชื่อ-นามสกุล 2. ที่อยู่ปัจจุบัน/ ที่อยู่ตามบัตรประชาชน 3. หมายเลขโทรศัพท์ 4. อีเมล 5. เสี่ยง
ผู้เอาประกันภัย	<u>ประกันภัยรถยนต์</u> 1. ชื่อ-นามสกุล 2. เลขบัตรประจำตัวประชาชน 3. ที่อยู่ปัจจุบัน/ ที่อยู่ตามบัตรประชาชน 4. วันเดือนปีเกิด 5. หมายเลขโทรศัพท์ 6. อีเมล 7. เพศ 8. อายุ 9. อาชีพ 10. สัญชาติ 11. เลขทะเบียนรถยนต์ 12. เลขที่หนังสือเดินทาง 13. เลขที่ใบอนุญาตขับขี่ 14. ประวัติสุขภาพ หรือคำถามเกี่ยวกับสุขภาพ 15. หมายเลขบัตรเครดิต 16. เลขบัญชีธนาคาร 17. ชื่อบัญชีธนาคาร 18. เลขที่กรมธรรม์ประกันภัย

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	ประเภทข้อมูลส่วนบุคคล (Personal Data)
	19. เสียง 20. ลายมือชื่อ 21. ภาพถ่าย 22. ภาพวิดีโอ <u>ประกันภัยทรัพย์สิน</u> 1. ชื่อ-นามสกุล 2. เลขบัตรประจำตัวประชาชน 3. ที่อยู่ปัจจุบัน/ ที่อยู่ตามบัตรประชาชน 4. สถานที่ตั้งทรัพย์สินที่เอาประกันภัย 5. วันเดือนปีเกิด 6. หมายเลขโทรศัพท์ 7. อีเมล 8. เพศ 9. สัญชาติ 10. ทรัพย์สินที่เอาประกันภัย เช่น สำเนาทะเบียนบ้าน โฉนดที่ดิน <u>ประกันภัยขนส่งทางทะเลและโลจิสติกส์</u> 1. ชื่อ-นามสกุล 2. เลขบัตรประจำตัวประชาชน 3. วันเดือนปีเกิด 4. หมายเลขโทรศัพท์ 5. อีเมล 6. เพศ 7. สัญชาติ 8. ข้อมูลยานพาหนะที่เอาประกันภัย เช่น สำเนาทะเบียนรถยนต์ <u>ประกันภัยเบ็ดเตล็ด</u> 1. ชื่อ-นามสกุล 2. เลขบัตรประจำตัวประชาชน

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	ประเภทข้อมูลส่วนบุคคล (Personal Data)
	3. วัน เดือน ปีเกิด 4. หมายเลขโทรศัพท์ 5. อีเมล 6. เพศ 7. ทรัพย์สินที่เอาประกันภัย <u>ประกันภัยอุบัติเหตุและสุขภาพ</u> 1. ชื่อ-นามสกุล 2. เลขบัตรประจำตัวประชาชน/เลขที่หนังสือเดินทาง 3. ที่อยู่ปัจจุบัน/ ที่อยู่ตามบัตรประชาชน 4. วัน เดือน ปีเกิด 5. หมายเลขโทรศัพท์ 6. อีเมล 7. เพศ 8. อาชีพ และสถานที่ทำงาน 9. ลายมือชื่อผู้ทำธุรกรรม 10. เชื้อชาติ/สัญชาติ 11. ข้อมูลสุขภาพ 12. ข้อมูลส่วนบุคคลเกี่ยวกับความพิการ 13. ข้อมูลพันธุกรรม
ผู้รับประกันภัย	1. ชื่อ-นามสกุล 2. หมายเลขโทรศัพท์ 3. ความสัมพันธ์กับผู้เอาประกันภัย
ผู้จ่ายเงิน	1. ชื่อ-นามสกุล 2. อีเมล 3. หมายเลขโทรศัพท์ 4. หมายเลขบัตรเครดิต 5. เลขบัญชีธนาคาร

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	ประเภทข้อมูลส่วนบุคคล (Personal Data)
	6. ชื่อบัญชีธนาคาร

ข้อสังเกต

- 1) การจะพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลหรือไม่นั้น ต้องพิจารณาถึงสภาพของข้อมูลส่วนบุคคลและบริบทของการประมวลผลข้อมูลส่วนบุคคลด้วย กล่าวคือ ข้อมูลบางอย่างหากถูกเก็บรวบรวมไว้แยกจากข้อมูลอื่น ๆ ก็จะสามารถระบุตัวบุคคลได้ แต่หากรวมกับข้อมูลอื่น ๆ จะทำให้สามารถระบุตัวบุคคลได้ไม่ว่าจะทางตรงหรือทางอ้อม เช่น อายุ เพศ ศาสนา อาชีพ หากบริษัทแยกเก็บข้อมูลส่วนบุคคลเหล่านี้เป็นชุดข้อมูลเดี่ยว ๆ ข้อมูลเหล่านี้ก็จะไม่สามารถระบุตัวบุคคลได้
- 2) ข้อมูลที่เกี่ยวกับนิติบุคคลบางกรณีอาจเป็น “ข้อมูลส่วนบุคคล” ได้ เช่น หนังสือรับรองบริษัทที่มีรายชื่อกรรมการบริษัทหรือรายชื่อผู้ถือหุ้นบริษัท
- 3) ประเภทของข้อมูลส่วนบุคคลที่จะถูกจัดเก็บหรือประมวลผลนั้น เป็นไปตามความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของแต่ละบริษัท เช่น ข้อมูลเสียงของผู้เอาประกันภัย หากบริษัทมีการเสนอขายผลิตภัณฑ์ประกันภัยผ่านทางโทรศัพท์ บริษัทก็จำเป็นต้องบันทึกและเก็บรักษาไฟล์เสียงสนทนาของผู้เสนอขายและผู้เอาประกันภัย/ผู้มุ่งหวังไว้ตามที่สำนักงาน คปภ. กำหนด

ตัวอย่างประเภทข้อมูลส่วนบุคคลที่ระบุตัวบุคคลได้โดยตรงและโดยอ้อม

ข้อมูลส่วนบุคคล	ระบุตัวบุคคลได้โดยตรง	ระบุตัวบุคคลได้โดยอ้อม
ชื่อ-นามสกุล	✓	
หมายเลขโทรศัพท์		✓
ที่อยู่		✓
อีเมล		✓
เลขทะเบียนรถยนต์		✓
เลขบัตรประจำตัวประชาชน	✓	
เลขที่หนังสือเดินทาง	✓	
เลขที่ใบอนุญาตขับขี่	✓	
ประวัติสุขภาพ หรือคำถามเกี่ยวกับสุขภาพ		✓
เพศ		✓
อายุ		✓
อาชีพ		✓
สัญชาติ		✓
หมายเลขบัตรเครดิต	✓	
เลขบัญชีธนาคาร	✓	
ชื่อบัญชีธนาคาร	✓	
วัน เดือน ปีเกิด		✓
เลขที่กรมธรรม์ประกันภัย		✓
แบบพิมพ์ลายนิ้วมือ	✓	

นอกจากข้อมูลส่วนบุคคลแล้ว พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลยังมีการกำหนดข้อมูลส่วนบุคคลไว้อีกประเภทหนึ่ง เรียกว่า “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” โดยที่ มาตรา 26 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดว่า ข้อมูลอันเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ รวมถึงข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการกำหนด ถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ตัวอย่างข้อมูลส่วนบุคคลที่มีความอ่อนไหวของธุรกิจประกันวินาศภัย ได้แก่

1. ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติหรือเผ่าพันธุ์ เช่น คำตอบเกี่ยวกับเชื้อชาติบนใบสมัครงาน ข้อมูลเชื้อชาติบนประวัติย่อ (CV) ของผู้สมัครงาน
2. ข้อมูลส่วนบุคคลเกี่ยวกับความพิการ เช่น คำตอบเรื่องความพิการในใบสมัครงาน ในใบคำขอเอาประกันภัย ข้อมูลความพิการบนบัตรประจำตัวคนพิการ
3. ข้อมูลส่วนบุคคลเกี่ยวกับพฤติกรรมทางเพศ
4. ข้อมูลสภาพแรงงาน
5. ข้อมูลสุขภาพ เช่น ประวัติสุขภาพ แบบตอบคำถามสุขภาพ คำตอบเกี่ยวกับโรคประจำตัว
6. ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา และข้อมูลจำลองลายนิ้วมือ
7. ประวัติอาชญากรรม

1.2.1.1 ข้อยกเว้นการบังคับใช้ พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล

มาตรา 4 แห่ง พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคลได้กำหนดกิจกรรมหรือลักษณะการประมวลผลข้อมูลส่วนบุคคลบางประการที่ได้รับยกเว้นไม่ต้องตกอยู่ภายใต้ พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล ดังนี้

“มาตรา 4⁵ พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

⁵ มาตรา 4 พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการสิทธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการแล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจกรรมใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (2) (3) (4) (5) และ(6) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย”

จากบทบัญญัติข้างต้น จะเห็นว่าแม้กิจกรรมที่ระบุในมาตรา 4 จะได้รับการยกเว้นไม่ต้องดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล แต่ตามมาตรา 4 วรรคท้าย กำหนดให้การประมวลผลข้อมูลส่วนบุคคลขององค์กรที่เกี่ยวข้องข้างต้นต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามมาตรฐานด้วย

ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่บุคคล หรือองค์กรตามมาตรา 4 ต้องปฏิบัติตามนั้น ให้เป็นไปตามที่คณะกรรมการกำหนด

สำหรับบริษัท เนื่องจากการประมวลผลข้อมูลส่วนบุคคลส่วนมากของบริษัท เป็นไปเพื่อการประกอบธุรกิจประกันวินาศภัย เช่น การเสนอขายผลิตภัณฑ์ประกันภัย การพิจารณารับประกันภัย การพิจารณาและการจ่ายค่าสินไหมทดแทน เป็นต้น ดังนั้น จะเห็นว่าการประมวลผลข้อมูลส่วนบุคคลของบริษัท จะไม่ได้รับการยกเว้นตาม (1) – (6) ตามมาตรา 4 นี้

ตัวอย่างการดำเนินการที่ได้รับการยกเว้นไม่อยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เช่น การส่งภาพถ่ายเพื่อนให้กับคนในครอบครัวตนเอง เช่นนี้ เป็นการประมวลผลข้อมูลส่วนบุคคลที่ใช้เพื่อประโยชน์ส่วนตน หรือกรณีที่ศาลต้องใช้ข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุลของคุณความ หรือพยานในคดีในการพิจารณาคดีของศาล

1.2.2 ขอบเขตการบังคับใช้ตามหลักดินแดน

ตามมาตรา 5 พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์เกี่ยวกับการใช้บังคับ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล ตามหลักดินแดน ดังต่อไปนี้

“มาตรา 5 พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า การเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผล ข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า จะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร”

จากบทบัญญัติข้างต้น สามารถสรุปหลักเกณฑ์การบังคับใช้ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล ตามหลักดินแดนได้ ดังนี้

1.2.2.1 กรณีผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในประเทศไทย (มาตรา 5 วรรค 1)

ตามหลักเกณฑ์นี้มีข้อพิจารณาเพียงประการเดียวว่าการประมวลผลข้อมูลส่วนบุคคลจะต้องตกอยู่ในบังคับของ พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคลหรือไม่ คือการพิจารณาที่ตั้งหรือที่อยู่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า เพียงแค่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในประเทศไทย แม้ว่าการประมวลผลข้อมูลส่วนบุคคลจะเกิดนอกประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กำหนดใน พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล นอกจากนั้นแล้ว การพิจารณาหลักเกณฑ์ข้อนี้ ไม่จำเป็นต้องพิจารณาถึงสัญชาติหรือที่อยู่ของเจ้าของข้อมูลส่วนบุคคลด้วย

ตัวอย่าง

บริษัทที่ตั้งอยู่ในประเทศไทย และมีการประมวลผลข้อมูลส่วนบุคคลของบุคคลต่าง ๆ เช่น ผู้มุ่งหวังลูกค้า คู่ค้า ผู้ขายสินค้าหรือผู้ให้บริการ (Vendors/Suppliers) และพนักงาน ดังนั้น การประมวลผลข้อมูลส่วนบุคคลของบริษัทจะต้องดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

1.2.2.2 กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกประเทศไทย (มาตรา 5 วรรค 2)

จากบทบัญญัติมาตรา 5 วรรค 2 จะเห็นได้ว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีการกำหนดขอบเขตการบังคับใช้กฎหมายนอกราชอาณาจักร (Extraterritorial Scope) เอาไว้ ซึ่งโดยทั่วไป กฎหมายที่ออกในประเทศใด มักจะมีผลบังคับใช้แค่ภายในประเทศนั้น ๆ เท่านั้น แต่ในบางกรณี กฎหมายอาจกำหนดให้มีผลบังคับใช้นอกราชอาณาจักรเป็นกรณีพิเศษเพื่อวัตถุประสงค์ของกฎหมายนั้น ๆ เป็นการเฉพาะ ดังเช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ ซึ่งหลักการ Extraterritorial Scope ที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ สอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ เช่น GDPR⁶ ซึ่งเป็นกฎหมายต้นแบบของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ด้วย

อย่างไรก็ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มิได้มุ่งหวังให้ทุกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทยต้องตกอยู่ภายใต้การบังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แต่กำหนดให้เพียงลักษณะกิจกรรมบางอย่างเท่านั้นที่ต้องอยู่ในบังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ลักษณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทยที่จะอยู่ภายใต้บังคับของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีดังนี้

1) ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศไทย

2) การเก็บรวบรวม ใช้ หรือเปิดเผยเป็นไปเพื่อกิจกรรมดังต่อไปนี้

(ก) การเสนอขายสินค้า หรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร ทั้งนี้ ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(ข) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

⁶ Article 3 of the GDPR

การเสนอขายสินค้า หรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร

หลักเกณฑ์สำคัญในการพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลเพื่อการเสนอขายสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลในไทยต้องตกอยู่ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือไม่ คือ การมุ่งหมายที่จะเสนอขายสินค้าหรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลในประเทศไทย (Targeting) กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่มีเจตนาหรือตั้งใจ “มุ่งหมาย” ที่จะเสนอขายสินค้าหรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศไทยเท่านั้น จึงจะต้องอยู่ภายใต้การบังคับใช้ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ในการพิจารณาว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลมุ่งหมายที่จะเสนอขายสินค้าหรือบริการให้กับเจ้าของข้อมูลส่วนบุคคลในไทยหรือไม่นั้น ต้องพิจารณาจากพฤติการณ์หลาย ๆ อย่าง ในกิจกรรมการเสนอขายสินค้าหรือบริการนั้น ๆ เช่น ภาษา สกุลเงิน หรือรูปแบบสินค้าหรือบริการ การใช้ Domain Name ที่เป็นของประเทศไทย อาทิ .th

ตัวอย่าง

บริษัทนายหน้าประกันภัยตั้งอยู่ที่ประเทศจีน เปิดเว็บไซต์เสนอขายประกันภัยอุบัติเหตุการเดินทางให้กับบุคคลที่จะเดินทางจากประเทศไทยไปประเทศจีน โดยเว็บไซต์สามารถเลือกภาษาเป็นภาษาไทยได้ เช่นนี้ แม้บริษัทนายหน้าประกันนั้นจะตั้งอยู่ในประเทศจีน แต่การที่เสนอขายผลิตภัณฑ์ประกันการเดินทางให้บุคคลที่จะเดินทางจากประเทศไทยไปประเทศจีน และมีการเปิดเว็บไซต์เป็นภาษาไทย สามารถแสดงให้เห็นได้ว่าบริษัทนายหน้าประกันนั้นมีเจตนามุ่งหมายที่จะเสนอขายผลิตภัณฑ์ประกันภัยให้กับคนที่อยู่ในประเทศไทย

(ข) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

ในการพิจารณาว่ากรณีใดเป็นการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดในประเทศไทย-แนวทางการพิจารณาของ GDPR สำหรับการเฝ้าติดตามพฤติกรรมที่จะทำให้ตกอยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ต้องเป็นกรณีที่มีการเฝ้าติดตามพฤติกรรมมีลักษณะดังต่อไปนี้

- 1) มีเจตนามุ่งหมายที่จะเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลในประเทศไทย
- 2) มีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นไปเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่ง (โดยเฉพาะอย่างยิ่งการติดตามพฤติกรรมเพื่อการตลาด)

ทั้งนี้ การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลตามแนวทางการพิจารณาของ The European Data Protection Board (EDPB) ไม่ได้จำกัดเฉพาะการเฝ้าติดตามผ่านทางอินเทอร์เน็ต แต่รวมถึงการเฝ้าติดตามพฤติกรรมผ่านอุปกรณ์ หรือช่องทางออนไลน์อื่น ๆ ด้วย⁷

1.3 การจัดการข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีผลบังคับใช้

ก่อนที่จะมีร่างและประกาศใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล การดำเนินการต่าง ๆ ของผู้ประกอบการเกี่ยวข้องเกี่ยวกับข้อมูลส่วนบุคคลตามความหมายที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อยู่แล้ว โดยเฉพาะอย่างยิ่งภาคธุรกิจที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก เช่น ภาคธุรกิจการเงิน การธนาคาร การประกันภัย การลงทุน หรือธุรกิจที่เกี่ยวข้องกับข้อมูลสารสนเทศ ดังนั้น เมื่อมีการประกาศใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ก็ย่อมส่งผลกระทบต่อผู้ประกอบการต่าง ๆ โดยตรง เนื่องจากผู้ประกอบการจะต้องดำเนินการเตรียมความพร้อม รวมถึงจัดการกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมมาก่อนที่ พ.ร.บ. จะมีผลบังคับใช้ ดังนั้น เพื่อไม่ให้เป็นการอุปสรรคต่อการดำเนินธุรกิจของผู้ประกอบการมาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จึงได้กำหนดขึ้นตอนหรือหลักเกณฑ์การจัดการข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จะมีผลบังคับใช้

1.3.1 ข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อนวันที่ พ.ร.บ. มีผลใช้บังคับ

หลักเกณฑ์การจัดการกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับถูกกำหนดในมาตรา 95 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ดังนี้

“มาตรา 95 ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้น ต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่ง ให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้”

ก่อนที่จะพิจารณาหลักเกณฑ์ในการจัดการข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับตามแต่ละกรณีที่กำหนดในมาตรา 95 ข้างต้น บริษัทต้องพิจารณาก่อน

⁷ หน้า 17, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

ว่า ข้อมูลใดบ้างเป็นข้อมูลที่เก็บรวบรวมก่อนวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับ หรือวันใดที่เป็นวันที่ “...พระราชบัญญัตินี้ใช้บังคับ...” ตามมาตรา 95 ข้างต้น

เนื่องจากมาตรา 95 เป็นหนึ่งในบทบัญญัติที่จะมีผลใช้บังคับในวันที่ 1 มิถุนายน 2565 ดังนั้น คำว่า “...พระราชบัญญัตินี้ใช้บังคับ...” ตามความหมายของมาตรา 95 จึงหมายถึงวันที่ 1 มิถุนายน 2565 (ไม่ใช่วันถัดจากวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลประกาศในราชกิจจานุเบกษา ซึ่งเป็นวันที่ 28 พฤษภาคม 2562)

1.3.2 หลักเกณฑ์การจัดการข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อนวันที่ พ.ร.บ. มีผลใช้บังคับ

หลักการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ใช้บังคับ ให้เก็บและใช้ได้ต่อไปได้ โดยมีเงื่อนไขและหลักเกณฑ์การดำเนินการ ดังนี้

- 1) เก็บรวบรวมและใช้ตามวัตถุประสงค์เดิม
- 2) มีการกำหนดช่องทางในการเพิกถอนความยินยอม
- 3) มีการประชาสัมพันธ์ช่องทางการเพิกถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ

การที่บริษัทจะเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้ต่อไปได้นั้น การเก็บรวบรวม และการใช้นั้นต้องเป็นไปตามวัตถุประสงค์เดิมของการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้น ๆ

ดังนั้น เพื่อการเก็บรวบรวมข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิมต่อไป สิ่งที่ต้องดำเนินการ มีดังนี้

- 1) ระบุว่าข้อมูลส่วนบุคคลใดบ้างเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมมาก่อนวันที่ พ.ร.บ. มีผลใช้บังคับ ทั้งฉบับ (วันที่ 1 มิถุนายน 2565)
- 2) ระบุเจ้าของข้อมูลส่วนบุคคล
- 3) ระบุวัตถุประสงค์เดิมของบริษัทในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล แต่ละประเภทข้อมูลส่วนบุคคล และแต่ละเจ้าของข้อมูลส่วนบุคคล

เมื่อบริษัทดำเนินการตามที่ระบุข้างต้นแล้ว บริษัทควรจัดทำเอกสารเป็นลายลักษณ์อักษร หรือบันทึกผลการดำเนินการดังกล่าวไว้ในรูปแบบอิเล็กทรอนิกส์เพื่อเป็นหลักฐาน เพื่อป้องกันการเกิดข้อโต้แย้งเกี่ยวกับการเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับ

ตัวอย่าง

1. ระบุว่าข้อมูลส่วนบุคคลใดบ้างเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมมาก่อนวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับ (ก่อนวันที่ 1 มิถุนายน 2565) บริษัท เอ เก็บรวบรวมข้อมูลส่วนบุคคลของนาย ก. ลูกค้าไว้ ดังนี้
 - ชื่อ – นามสกุล
 - เพศ
 - หมายเลขโทรศัพท์
 - อายุ
 - ที่อยู่
 - อาชีพ
 - อีเมล
 - หมายเลขบัตรเครดิต
 - เลขทะเบียนรถยนต์
 - เลขบัญชีธนาคาร
 - เลขบัตรประจำตัวประชาชน
 - ชื่อบัญชีธนาคาร
 - เลขที่หนังสือเดินทาง
 - วันเดือนปีเกิด
 - เลขที่ใบอนุญาตขับขี่
 - เลขที่กรมธรรม์ประกันภัย
 - อายุ
 - เสี่ยง
2. ระบุเจ้าของข้อมูลส่วนบุคคล – ในกรณีนี้เจ้าของข้อมูลส่วนบุคคล คือ นาย ก. ลูกค้า
3. ระบุวัตถุประสงค์เดิมของบริษัทในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลแต่ละประเภทข้อมูลส่วนบุคคลและแต่ละประเภทเจ้าของข้อมูลส่วนบุคคล – บริษัท เอ เก็บรวบรวมข้อมูลส่วนบุคคลของนาย ก. เพื่อวัตถุประสงค์ดังต่อไปนี้
 - เพื่อพิจารณารับประกันภัย
 - เพื่อรับประกันภัย
 - เพื่อให้บริการต่าง ๆ ที่เกี่ยวข้องกับการประกันภัย
 - เพื่อประโยชน์เกี่ยวกับการดำเนินการจ่ายค่าสินไหมทดแทน
 - เพื่อการพิสูจน์ยืนยันตัวตนก่อนเข้าทำสัญญาประกันภัย
 - เพื่อเสนอขายผลิตภัณฑ์ประกันภัยที่เหมาะสม
 - เพื่อวิเคราะห์และปรับปรุงผลิตภัณฑ์
 - เพื่อการดำเนินการทางการตลาดอื่น ๆ
 - เพื่อการทำประกันภัยต่อ

ดังนั้น ตั้งแต่ 1 มิถุนายน 2565 บริษัท เอ จะยังสามารถเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลของนาย ก. ตามที่ระบุข้างต้นเพื่อการดำเนินการตามวัตถุประสงค์เดิมข้างต้นได้

1.3.3 ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอม

เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ได้กำหนดวิธีการ หรือรูปแบบในการให้เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมไว้ ดังนั้น วิธีการและช่องทางที่บริษัทต้องจัดให้มี เพื่อให้เจ้าของข้อมูลส่วนบุคคลดำเนินการเพิกถอนความยินยอมได้นั้นย่อมขึ้นอยู่กับข้อกำหนดของแต่ละบริษัท โดยในการกำหนดวิธีการถอนความยินยอมนั้น บริษัทควรพิจารณาประเด็นดังต่อไปนี้

- 1) บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลประเภทใดบ้าง
- 2) บริษัทใช้ช่องทางการสื่อสารกับเจ้าของข้อมูลส่วนบุคคลอย่างไรบ้าง เช่น บริษัท สื่อสารกับลูกค้าผ่านทาง SMS, Website, Facebook Page, Line Official อีเมล และทางโทรศัพท์

ในกรณีที่บริษัทมีการเก็บข้อมูลส่วนบุคคลโดยอาศัยฐานความยินยอม บริษัทอาจกำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถขอเพิกถอนความยินยอมได้ตามช่องทางการสื่อสารเดิมที่บริษัทใช้กับเจ้าของข้อมูลส่วนบุคคลในแต่ละประเภท หากเดิมบริษัทมีช่องทางการติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคลหลายช่องทางบริษัท อาจกำหนดให้ช่องทางการเพิกถอนความยินยอมเป็นไปเพียงช่องทางใดช่องทางหนึ่งเท่านั้นก็ได้ ทั้งนี้ ขึ้นอยู่กับระบบการจัดการข้อมูลส่วนบุคคลของบริษัท

1.3.4 ผู้ควบคุมข้อมูลส่วนบุคคลต้องเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

เมื่อมีการกำหนดระบบหรือขั้นตอนในการให้เจ้าของข้อมูลส่วนบุคคลยกเลิกความยินยอมได้แล้ว บริษัทจะต้องประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวิธีการหรือขั้นตอนการแจ้งยกเลิกความยินยอมนั้นด้วย

ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดเงื่อนไขเพียงว่าให้บริษัท “เผยแพร่ประชาสัมพันธ์” ช่องทางการเพิกถอนความยินยอม ดังนั้น บริษัทจะดำเนินการเผยแพร่ประชาสัมพันธ์โดยวิธีการใดก็ได้ โดยคำนึงถึงช่องทางที่จะทำให้เจ้าของข้อมูลส่วนบุคคลสามารถรับรู้ถึงวิธีการในการเพิกถอนความยินยอมที่กำหนดไว้ได้

บริษัทอาจดำเนินการประชาสัมพันธ์ช่องทางการเพิกถอนความยินยอมแบบ Passive เช่น การประกาศเผยแพร่บนหน้าเว็บไซต์ของบริษัทของตน หรืออาจดำเนินการเผยแพร่ประชาสัมพันธ์แบบ Proactive ก็ได้ เช่น ส่งข้อความสั้น (SMS) อีเมล หรือจดหมายให้กับเจ้าของข้อมูลส่วนบุคคลรายบุคคล เป็นต้น

ข้อพึงระวัง

หลักเกณฑ์และวิธีการข้างต้นใช้ได้กับกรณีการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อน พ.ร.บ. มีผลใช้บังคับเท่านั้น แต่จะไม่รวมถึงการเปิดเผยข้อมูลส่วนบุคคลและการดำเนินการอื่น ๆ กับข้อมูลส่วนบุคคล ซึ่งเป็นกรณีที่ต้องปฏิบัติตามข้อกำหนดของเรื่องนั้น ๆ ตามที่กำหนดไว้ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ตามที่จะพูดถึงในข้อ 1.3.5

1.3.5 กรณีการเปิดเผย และการดำเนินการอื่นเกี่ยวกับข้อมูลส่วนบุคคลที่เก็บรวบรวมก่อนวันที่ พ.ร.บ. มีผลใช้บังคับต่อไป

ตามมาตรา 95 วรรค 2 กำหนดว่า “การเปิดเผยและการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่ง ให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้”

หลักการตามมาตรา 95 วรรค 2 กำหนดไว้สำหรับการเปิดเผยและการดำเนินการอื่นที่ไม่ใช่การเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลที่มีการเก็บมาก่อน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับตามที่ได้อธิบายไว้ในส่วนที่แล้ว

ในการเปิดเผย หรือการดำเนินการอื่นใดกับข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการตามข้อกำหนดที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เช่น การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ การปฏิบัติตามหน้าที่อื่น ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

1.3.6 การพิจารณาความหมายของคำว่า “การเปิดเผย หรือการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่ง”

เนื่องจากมาตรา 95 วรรค 1 เป็นเรื่องของหลักเกณฑ์ในเรื่องการเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม ดังนั้น คำว่า “การเปิดเผย หรือการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่ง” จึงอาจตีความได้ว่าหมายรวมถึงกรณีดังต่อไปนี้

- 1) การเก็บรวบรวมและใช้นอกเหนือวัตถุประสงค์เดิม
- 2) การเปิดเผยข้อมูลส่วนบุคคล

ในกรณีที่บริษัทเปิดเผยข้อมูลส่วนบุคคลให้กับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอื่นที่ผู้รับข้อมูลส่วนบุคคล หรือมีข้อมูลส่วนบุคคลที่บริษัทจะเปิดเผยให้อยู่ในความครอบครองของผู้รับอยู่แล้วนั้น อาจตีความได้ว่า กรณีนี้เป็นการที่บริษัทซึ่งเป็นผู้ส่งข้อมูลและผู้รับข้อมูล ต่างก็เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิมของตนอยู่แล้ว ดังนั้น ในกรณีนี้จึงควรตกอยู่ภายใต้หลักเกณฑ์ตาม

มาตรา 95 วรรค 1 ดังรายละเอียดข้างต้น กล่าวคือ ทั้งบริษัทผู้ส่งข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลจะสามารถดำเนินการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่ตนมีอยู่เดิม รวมถึงส่งหรือรับข้อมูลที่ต่างฝ่ายต่างมีระหว่างกันได้ตามวัตถุประสงค์เดิม และดำเนินการตามที่มาตรา 95 วรรค 1 กำหนด

กรณีการเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 95 วรรค 2 นี้ ควรจำกัดเพียงกรณีการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สามเป็นครั้งแรก ซึ่งบุคคลที่สามดังกล่าวยังไม่เคยมีข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลดังกล่าวอยู่ก่อนหน้านั้น

- 3) การดำเนินการเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
- 4) การดำเนินการเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล
- 5) การจัดให้มีมาตรฐานการรักษาความปลอดภัยของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

1.3.7 การดำเนินการ “ให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้”

ในการดำเนินการให้เป็นไปตามบทบัญญัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล นั้น หมายถึงการที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ต้องพิจารณาและดำเนินการตามหลักเกณฑ์และข้อกำหนดที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดในการเปิดเผยและดำเนินการอื่น ๆ กับข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมก่อนวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล นี้มีผลใช้บังคับ

หากบริษัทมีการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สามโดยไม่เข้าลักษณะของการดำเนินการตามมาตรา 95 วรรค 1 ดังอธิบายข้างต้น และเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานความยินยอม บริษัทยังคงมีหน้าที่ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและมีหน้าที่แจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และหากเป็นการเปิดเผยข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทก็มีหน้าที่ต้องจัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวด้วย

1.4 การปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอื่น

ในกรณีการปรับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอื่นที่เกี่ยวข้องนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์ในการปรับใช้กฎหมายไว้ดังนี้

“มาตรา 3 ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(2) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี”

จากบทบัญญัติมาตรา 3 ข้างต้น สามารถสรุปหลักเกณฑ์ในการปรับใช้กฎหมายได้ ดังนี้

1.4.1 กรณีที่ให้บังคับใช้ทั้งกฎหมายเฉพาะ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

บทบัญญัติกฎหมายในเรื่องดังต่อไปนี้ให้บังคับใช้ทั้งกฎหมายที่มีการกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ และใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ควบคู่เพิ่มเติมไปด้วยโดยที่ไม่จำกัดว่าบทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และบทบัญญัติในกฎหมายเฉพาะอื่นซ้ำกันหรือไม่

บทบัญญัติดังกล่าวรวมถึงบทบัญญัติในกรณี หรือเรื่องดังต่อไปนี้

1.4.1.1 บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บทบัญญัติในเรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนี้ หมายความว่าถึงบทบัญญัติในหมวด 2 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อันประกอบไปด้วย

ส่วนที่ 1 บททั่วไป (มาตรา 19-มาตรา 21) เป็นส่วนที่กำหนดเกี่ยวกับเรื่องหลักของการขอความยินยอมในกรณีทั่วไป การขอความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ และหลักในการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์

ส่วนที่ 2 การเก็บรวบรวมข้อมูล (มาตรา 22 – มาตรา 26) บทบัญญัติในส่วนนี้จะกล่าวถึงฐานอันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลประเภทที่ระบุไว้เป็นพิเศษหรือเรียกว่า “ข้อมูลที่มีความอ่อนไหว” (Sensitive Personal Data) รวมถึงหลักเกณฑ์เกี่ยวกับการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

ส่วนที่ 3 การใช้และการเปิดเผยข้อมูลส่วนบุคคล (มาตรา 27 – มาตรา 29) บทบัญญัติส่วนนี้กำหนดหลักเกณฑ์ในเรื่องการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

1.4.1.2 บทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

เป็นบทบัญญัติที่กำหนดในหมวด 3 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ตั้งแต่มาตรา 30 ถึง มาตรา 42 ซึ่งบทบัญญัติส่วนนี้กำหนดในเรื่องของสิทธิของเจ้าของข้อมูลส่วนบุคคล การเรียกร้องตามสิทธิหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงคุณสมบัติและหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer (DPO))

1.4.1.3 บทกำหนดโทษที่เกี่ยวข้อง

บทกำหนดโทษที่เกี่ยวข้องนี้ หมายถึงบทบัญญัติที่เกี่ยวกับความรับผิด และโทษที่เกี่ยวข้องกับการกระทำความผิด ได้แก่

หมวด 6 ความรับผิดทางแพ่ง (มาตรา 77 – มาตรา 78) กำหนดในเรื่องหลักของความรับผิดทางแพ่งเกี่ยวกับการไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมถึงการกำหนดให้ศาลมีอำนาจพิจารณาให้บุคคลจ่ายค่าสินไหมทดแทนเชิงลงโทษได้

หมวด 7 บทกำหนดโทษ โดยแบ่งออกเป็น 2 ส่วนคือ ส่วนที่ 1 โทษอาญา (มาตรา 79 – มาตรา 81) และส่วนที่ 2 โทษทางปกครอง (มาตรา 82 – มาตรา 90)

1.4.2 กรณีที่ใช้บังคับตามบทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- 1) บทบัญญัติเกี่ยวกับการร้องเรียน
- 2) บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล
- 3) บทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ และ
- 4) บทกำหนดโทษที่เกี่ยวข้อง

บทบัญญัติดังกล่าวอาจรวมถึงบทบัญญัติดังต่อไปนี้

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 8 – มาตรา 18) - ในหมวดนี้จะมีการระบุ กฎเกณฑ์ คุณสมบัติ รวมถึงอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 43 – มาตรา 70) - บทบัญญัติส่วนนี้กำหนดให้มีการตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อำนาจหน้าที่ของสำนักงาน รวมถึง คุณสมบัติของพนักงานเจ้าหน้าที่ของสำนักงาน

หมวด 5 การร้องเรียน (มาตรา 71 – มาตรา 76) - บทบัญญัติส่วนนี้กำหนดในเรื่องขั้นตอนการ ร้องเรียนเกี่ยวกับการฝ่าฝืน หรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ต่อสำนักงาน รวมถึงกำหนด ขั้นตอนในการพิจารณาเรื่องร้องเรียนดังกล่าว

นอกจากนั้น ยังรวมถึงบทบัญญัติที่เกี่ยวกับโทษที่เกี่ยวข้องกับเรื่องข้างต้นด้วย โดยบทบัญญัตินี้กำหนดให้บังคับตามบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเท่านั้น หากเป็นกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่อง ร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอ เท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่น คำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

บทที่ 2 หลักการพื้นฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.1 ความชอบด้วยกฎหมาย และความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคล

2.1.1 หลักความชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawfulness Principle)

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้การเก็บรวบรวม ใช้ และประมวลผลข้อมูลส่วนบุคคลต้องได้รับความยินยอม หรือต้องอยู่บนฐานโดยชอบด้วยกฎหมายอื่น ตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดไว้ในมาตรา 24 และมาตรา 26 จึงจะสามารถทำได้

ฐานโดยชอบด้วยกฎหมาย (Lawful Basis) สำหรับการประมวลผลข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ถูกกำหนดไว้ต่างกัน ดังนี้

- 1) ฐานโดยชอบด้วยกฎหมายของข้อมูลส่วนบุคคลทั่วไป ตามมาตรา 24 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
 - ฐานสัญญา
 - ฐานความยินยอม
 - ฐานประโยชน์ที่สำคัญต่อชีวิต
 - ฐานหน้าที่ตามกฎหมาย
 - ฐานภารกิจของรัฐ
 - ฐานประโยชน์อันชอบธรรม
 - ฐานจดหมายเหตุ/ วิจัย/ สถิติ
- 2) ฐานโดยชอบด้วยกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ตามมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
 - ฐานความยินยอม (โดยชัดแจ้ง)
 - ฐานประโยชน์ที่สำคัญต่อชีวิต

- ฐานเพื่อการดำเนินการของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร
- ฐานข้อมูลที่เปิดเผยโดยสาธารณะโดยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล
- ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับสิทธิเรียกร้อง
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคม
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับเวชศาสตร์ป้องกัน หรือ อาชีวศาสตร์
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ

รายละเอียดในการประมวลผลข้อมูลส่วนบุคคลในแต่ละกรณีจะมีการอธิบายต่อไปใน **บทที่ 5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล**

นอกจากฐานโดยชอบด้วยกฎหมายดังระบุไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลแล้ว ตามแนวทางของ GDPR กำหนดว่า หลักความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคลนี้ ต้องพิจารณาความชอบด้วยกฎหมายตามกฎหมายอื่นด้วย กล่าวคือ นอกจากการประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ฝ่าฝืนบทบัญญัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลแล้ว การประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ฝ่าฝืนบทบัญญัติตามกฎหมายอื่น ๆ ด้วย เช่น ต้องไม่ประมวลผลข้อมูลส่วนบุคคลที่ทำให้เกิดการละเมิดลิขสิทธิ์ หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ในกรณีนี้อาจหมายความว่ากฎหมายประกันภัยด้วย⁸

2.1.2 หลักความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคล (Transparency Principle)

ในการประมวลผลข้อมูลส่วนบุคคลนั้น นอกจากจะต้องกระทำบนฐานโดยชอบด้วยกฎหมายแล้ว ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคลด้วย ความโปร่งใส (Transparency) นี้ หมายถึง ความชัดเจน การเปิดเผย และความซื่อตรง ในการ

⁸ What is Lawfulness, ICO, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>, accessed on April 6, 2020

ประมวลผลข้อมูลส่วนบุคคล ดังนั้น เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเกิดความโปร่งใส พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จึงกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบโดยต้องมีเนื้อหาอย่างน้อยตามที่มาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด ก่อนหรือขณะที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล

นอกจากนั้น ในกรณีที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวมมาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลก็อาจมีหน้าที่แจ้งการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น และแจ้งรายละเอียดตามที่กำหนดในมาตรา 23 ให้เจ้าของข้อมูลส่วนบุคคลทราบด้วย ทั้งนี้ ขึ้นอยู่กับลักษณะการเก็บรวบรวมข้อมูลส่วนบุคคล และฐานในการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ ด้วย เช่น หากข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมมาจากแหล่งอื่น ต้องอ้างอิงฐานความยินยอม บริษัทก็มีหน้าที่ต้องขอความยินยอม และแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบตามหลักเกณฑ์ที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (โปรดดูรายละเอียดในเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นในบทที่ 5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หัวข้อ 5.6 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น)

ตัวอย่าง

กรณีที่น่ายหนึ่ง ระบุชื่อ นางสาว เป็นผู้รับประโยชน์ในสัญญาประกันภัยอุบัติเหตุการเดินทางที่ทำกับบริษัท ซี เช่นนี้ บริษัท ซี เก็บรวบรวมข้อมูลส่วนบุคคลของนางสาวมาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลเอง แต่เนื่องจากการประมวลผลข้อมูลส่วนบุคคลของนางสาวนั้นเป็นไปเพื่อประโยชน์ในการดำเนินการเกี่ยวกับการจ่ายค่าสินไหมทดแทนตามกรมธรรม์ประกันภัยที่นายหนึ่ง เข้าทำกับบริษัท ซี การประมวลผลข้อมูลส่วนบุคคลของนางสาว จึงอยู่บนฐานประโยชน์อันชอบธรรม (ไม่ใช่ฐานสัญญาเนื่องจากนางสาวไม่ใช่คู่สัญญากับบริษัท ซี) ดังนั้น ในกรณีนี้บริษัท ซี ไม่ต้องดำเนินการขอความยินยอมและแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้นางสาว

2.2 ข้อจำกัดด้านวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

หลักในเรื่องข้อจำกัดด้านวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้น มีความเกี่ยวเนื่องกับหลักความโปร่งใส (Transparency) เนื่องจากหลักการนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ และประมวลผลตามที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเท่านั้น โดยใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีการกำหนดว่าในการขอความยินยอมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคลจะต้องแจ้งรายละเอียดเกี่ยวกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบด้วย⁹

นอกจากนั้น มาตรา 21 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ยังกำหนดขอบเขตของการประมวลผลข้อมูลส่วนบุคคลไว้ว่า การประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องทำภายใต้วัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลเท่านั้น การประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์เดิมจะกระทำไม่ได้ เว้นแต่ ได้แจ้งวัตถุประสงค์ใหม่และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว หรือการดำเนินการประมวลผลข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์เดิมนั้นมีบทบัญญัติกฎหมายอื่น รวมถึง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ให้กระทำได้

ตัวอย่างที่ 1

เดิมบริษัทแจ้งเจ้าของข้อมูลส่วนบุคคลเพียงว่า บริษัทจะประมวลผลข้อมูลส่วนบุคคลเพื่อการทำประกันภัย แต่ต่อมาบริษัทจะนำข้อมูลส่วนบุคคลไปใช้เพื่อดำเนินกิจกรรมทางการตลาด หากกิจกรรมทางการตลาดนั้นมีลักษณะที่อยู่ในความคาดหมายของเจ้าของข้อมูลส่วนบุคคล บริษัทอาจอ้างอิงฐานการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายได้ โดยอ้างอิงตามการทดสอบสามส่วน แต่หากกิจกรรมดังกล่าวมีลักษณะที่เกินความคาดหมายของเจ้าของข้อมูลส่วนบุคคล เช่นนี้ ถือได้ว่า บริษัทกระทำการนอกเหนือวัตถุประสงค์เดิมที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล บริษัทจึงไม่สามารถทำได้ เว้นแต่บริษัทได้ดำเนินการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อการตลาดในลักษณะดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลใหม่

ตัวอย่างที่ 2

จากตัวอย่างที่ 1 เดิมบริษัทแจ้งเจ้าของข้อมูลส่วนบุคคลเพียงว่า บริษัทจะประมวลผลข้อมูลส่วนบุคคลเพื่อการทำประกันภัย (อ้างอิงฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคล) ต่อมาเมื่อมีการรับประกันภัยแล้ว และมีการเรียกร้องค่าสินไหมทดแทนเกิดขึ้น บริษัทจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เอาประกันภัยเกี่ยวกับภัยที่เกิดขึ้นตามกรมธรรม์เพื่อพิจารณาการจ่ายค่าสินไหมทดแทน เช่นนี้ บริษัทไม่จำเป็นต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลใหม่แล้ว เนื่องจากการพิจารณาจ่ายค่าสินไหมทดแทนยังคงอยู่ในวัตถุประสงค์เดิมของการเก็บรวบรวมข้อมูลส่วนบุคคล กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลเพื่อการเรียกร้องค่าสินไหมทดแทนยังคงอยู่ในวัตถุประสงค์ของ “การรับประกันภัย”

⁹ มาตรา 19 และมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

2.3 ความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล

หลักการหนึ่งที่สำคัญใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และเป็นหลักการเบื้องต้นของการคุ้มครองข้อมูลส่วนบุคคลทั้งในประเทศไทยและต่างประเทศ¹⁰ คือ หลักในเรื่องความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล (Data Minimization) กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคลนั้นทำได้เท่าที่จำเป็น และจำกัดอยู่เพียงข้อมูลที่จำเป็นในการบรรลุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ¹¹ ดังนั้น บริษัทจะต้องกำหนดวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของบริษัททั้งหมดก่อน แล้วจึงจะสามารถพิจารณาและกำหนดได้ว่าข้อมูลใดจำเป็นในการประมวลผลข้อมูลส่วนบุคคล หากบริษัทพบว่าข้อมูลใดไม่จำเป็นในการประมวลผลเพื่อบรรลุวัตถุประสงค์ของบริษัท บริษัทก็ควรพิจารณาจัดการกับข้อมูลส่วนบุคคลดังกล่าวเพื่อลดความเสี่ยงในการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เช่น ดำเนินการลบหรือทำลาย หรือไม่เก็บรวบรวมข้อมูลส่วนบุคคลเหล่านั้น

ตัวอย่าง

เดิมบริษัทออกแบบใบสมัครเป็นตัวแทนประกันวินาศภัยให้ผู้สมัครต้องระบุรายละเอียดเกี่ยวกับส่วนสูง น้ำหนัก และบุคคลในครอบครัว ซึ่งบริษัทไม่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลดังกล่าวในการพิจารณารับบุคคลเข้าทำงานเป็นตัวแทนประกันวินาศภัยของบริษัท ดังนั้น บริษัทควรพิจารณาปรับเปลี่ยนรูปแบบของใบสมัครนั้น โดยลบคำถามเกี่ยวกับข้อมูลส่วนบุคคลที่ไม่จำเป็นต่อการรับสมัครตัวแทนประกันวินาศภัยออก เป็นต้น

2.4 ความถูกต้อง สมบูรณ์ และเป็นปัจจุบันของข้อมูลส่วนบุคคล

หลักในเรื่องความถูกต้อง สมบูรณ์ และเป็นปัจจุบันของข้อมูลส่วนบุคคล ถูกกำหนดไว้เป็นหน้าที่หนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ ในมาตรา 35 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนดว่า ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้ นอกจากนั้น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ยังกำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการทำให้ข้อมูลส่วนบุคคลของตนถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้เช่นกัน¹²

¹⁰ Article 5(1)(c) of the GDPR

¹¹ มาตรา 22 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

¹² มาตรา 35 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

2.5 ความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคล

หลักในเรื่องความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลนี้ปรากฏอยู่ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หลายมาตรา ดังนี้

มาตรา 22 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลได้เท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ซึ่งคำว่า “เท่าที่จำเป็น” นั้น อาจพิจารณาได้ทั้งแง่ของปริมาณ หรือประเภทข้อมูลส่วนบุคคล และในแง่ของระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลนั้น ๆ ด้วย

มาตรา 23 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลรวมถึงรายละเอียดเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล (ปัจจุบันสำนักงาน คปภ. หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องยื่นนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ที่ทำขึ้นเพื่อแจ้งรายละเอียดตามมาตรา 23 เพื่อให้สำนักงาน คปภ. อนุมัติ)

มาตรา 37(3) กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีระบบในการดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเหล่านั้น

ในส่วนของระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลนั้น ขึ้นอยู่กับความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลของแต่ละกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบริษัท โดยบริษัทอาจอ้างอิงระยะเวลาตามกฎหมาย หรือข้อกำหนด หรือความจำเป็นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ ได้ เช่น บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เอาประกันภัยในส่วนที่เกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงของลูกค้ายเป็นระยะเวลา 10 ปีนับแต่ที่มีการยุติความสัมพันธ์กับลูกค้า (ผู้เอาประกันภัย) เช่นนี้ บริษัทก็สามารถกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการตรวจสอบเพื่อทราบข้อเท็จจริงของลูกค้ายได้ 10 ปีนับแต่ที่มีการยุติความสัมพันธ์กับลูกค้า (ผู้เอาประกันภัย) ตามความจำเป็นเพื่อการปฏิบัติตามกฎหมาย (พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน)

2.6 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

หลักการหนึ่งที่สำคัญของการคุ้มครองข้อมูลส่วนบุคคลคือ มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้รับหลักการนี้มาจากกฎหมายต่างประเทศ และกำหนดให้หน้าที่ในการจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหนึ่งใน

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล¹³ และผู้ประมวลผลข้อมูลส่วนบุคคล¹⁴ โดยทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และนอกจากนั้นผู้ควบคุมข้อมูลส่วนบุคคลยังต้องคอยทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสมด้วย

ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ขึ้นอยู่กับการดำเนินการของแต่ละบริษัท และมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ/หรือ คณะกรรมการกำหนด

2.7 หลักการรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

หลักการในเรื่องความรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล หมายถึง การที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และสามารถแสดงให้เห็นถึงการปฏิบัติตามกฎหมายได้¹⁵ ซึ่งโดยมากสิ่งที่จะสามารถแสดงให้เห็นถึงดำเนินการตามที่กฎหมายกำหนดได้ คือ การจัดทำบันทึกการดำเนินการต่าง ๆ ไว้เป็นลายลักษณ์อักษร

การดำเนินการตามหลักการนี้สามารถทำได้โดยการดำเนินการตามหน้าที่ที่เกี่ยวข้องตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด เช่น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีการบันทึกการประมวลผลข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือทางอิเล็กทรอนิกส์¹⁶ ต้องมีกระบวนการดำเนินการแจ้งในกรณีที่เกิดการละเมิดข้อมูลส่วนบุคคล¹⁷ หรือจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม¹⁸ เป็นต้น

¹³ มาตรา 37(1) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹⁴ มาตรา 40(2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹⁵ What is accountability principle, ICO, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/>

¹⁶ มาตรา 39 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹⁷ มาตรา 37(4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹⁸ มาตรา 37(1) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

บทที่ 3 ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

3.1 ผู้ควบคุมข้อมูลส่วนบุคคล

3.1.1 ความหมายของผู้ควบคุมข้อมูลส่วนบุคคล

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

จากคำนิยามข้างต้น สามารถเข้าใจได้ว่าไม่ว่าจะเป็นบุคคลธรรมดา หรือนิติบุคคลย่อมสามารถมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลได้ หากบุคคลดังกล่าวมีอำนาจหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยพิจารณาแต่ละกิจกรรมการประมวลผลข้อมูลที่เกี่ยวข้อง

ข้อพิจารณาเบื้องต้น¹⁹

หากบริษัทมีลักษณะการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้ บริษัทถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล

- บริษัทเป็นผู้มีอำนาจตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใด
- บริษัทเป็นผู้มีอำนาจตัดสินใจว่าข้อมูลส่วนบุคคลนั้นนำมาใช้เพื่อวัตถุประสงค์ใด
- บริษัทเป็นผู้มีอำนาจตัดสินใจว่าจะเก็บข้อมูลส่วนบุคคลของบุคคลใด
- บริษัทเป็นผู้มีอำนาจตัดสินใจว่าจะกำหนดให้ผลของการประมวลผลข้อมูลนั้นเป็นอย่างไร
- บริษัทไม่ได้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของบุคคลอื่น หรือเป็นผู้แทนของบุคคลอื่น หรือองค์กรอื่น

ตัวอย่าง

บริษัทเก็บรวบรวมข้อมูลส่วนบุคคล ผ่านตัวแทนประกันวินาศภัยของบริษัท เพื่อนำข้อมูลดังกล่าวไปใช้ในการพิจารณาการรับประกันภัย ในกรณีดังกล่าวจะเห็นได้ว่า บริษัทมีอำนาจตัดสินใจในการเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคลของผู้มุ่งหวังเพื่อบริษัทเอง และในนามของบริษัทเองว่าจะพิจารณา

¹⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/>

ประกันภัย หรือกำหนดเบี้ยประกันภัยอย่างไร ในกรณีกิจกรรมการรับประกันภัยนี้ บริษัทเป็นผู้ควบคุมข้อมูลส่วนบุคคล (และตัวแทนประกันวินาศภัยของบริษัทถือว่าเป็นผู้ประมวลผลข้อมูลส่วนบุคคล – ตามที่จะอธิบายในหัวข้อถัดไป)

3.1.2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

1) หน้าที่ประมวลผลข้อมูลส่วนบุคคลตามฐานโดยชอบด้วยกฎหมาย²⁰

ในการดำเนินการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องพิจารณาก่อนเริ่มดำเนินการเสมอว่าการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ มีฐานโดยชอบด้วยกฎหมายรองรับหรือไม่ ซึ่งฐานในการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล นั้นถูกกำหนดไว้ในมาตรา 24 สำหรับข้อมูลส่วนบุคคลทั่วไป และมาตรา 26 สำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหว

หากการประมวลผลข้อมูลส่วนบุคคลต้องอ้างอิงฐานความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว โดยการขอความยินยอมจะต้องทำโดยชัดแจ้ง พร้อมระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นด้วย และวิธีการในการขอความยินยอมต้องเป็นไปตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดด้วย²¹ (โปรดดูรายละเอียดในเรื่องการขอความยินยอมในบทที่ 5 ของแนวปฏิบัติฉบับนี้)

2) หน้าที่ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่แจ้งเจ้าของข้อมูลส่วนบุคคล²²

ตามที่ได้อธิบายในเรื่องข้อจำกัดด้านวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (Purpose Limitation Principle) ในบทที่ 2 ของแนวปฏิบัติฉบับนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่แจ้งต่อเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้ง และได้รับความยินยอมในวัตถุประสงค์ใหม่ ก่อนทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ใหม่ หรืออาจประมวลผลข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ได้ในกรณีที่มีกฎหมายให้อำนาจกระทำได้

²⁰ มาตรา 24 และมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²¹ มาตรา 19 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²² มาตรา 21 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3) หน้าที่เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย²³

หน้าที่ในการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นนี้เป็นไปตามหลักในเรื่อง *ความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล (Data Minimization Principle)* ตามที่อธิบายในบทที่ 2 ของแนวปฏิบัติฉบับนี้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อการดำเนินการภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

4) หน้าที่แจ้งรายละเอียดตามที่กฎหมายกำหนดแก่เจ้าของข้อมูลส่วนบุคคล ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล²⁴

หน้าที่เกี่ยวกับเรื่องการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลนี้ เป็นไปตามหลัก *ความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคล (Transparency Principle)* กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลนั้น เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

- (ก) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่กฎหมายให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- (ข) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย หรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญารวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- (ค) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม
- (ง) ประเภทของบุคคล หรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- (จ) ข้อมูลเกี่ยวกับ สถานที่ติดต่อ และวิธีการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล และตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลด้วย (หากมี)
- (ฉ) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย

²³ มาตรา 22 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²⁴ มาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

5) หน้าที่ตรวจสอบให้แน่ใจว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางเพียงพอกรณีส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ²⁵

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องตรวจสอบให้แน่ใจว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางเพียงพอตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่การส่งหรือโอนข้อมูลส่วนบุคคลสามารถดำเนินการตามข้อยกเว้นในเรื่องมาตรฐานที่เพียงพอตามกรณีที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดได้

6) หน้าที่ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล²⁶

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลที่อนุญาตให้เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิของตนต่อผู้ควบคุมข้อมูลส่วนบุคคลไว้ดังนี้

- (ก) สิทธิในการเพิกถอนความยินยอม
- (ข) สิทธิในการได้รับแจ้งข้อมูล
- (ค) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- (ง) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- (จ) สิทธิในการลบข้อมูลส่วนบุคคล
- (ฉ) สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล
- (ช) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
- (ซ) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

หากการดำเนินการร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามเงื่อนไขที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธการร้องขอใช้สิทธินั้นได้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติตามคำขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

²⁵ มาตรา 28 และมาตรา 29 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²⁶ มาตรา 30 ถึง มาตรา 36 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

นอกจากสิทธิข้างต้น เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิยื่นข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลต่อคณะกรรมการผู้เชี่ยวชาญตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ด้วย²⁷

ทั้งนี้ ไม่ว่าข้อมูลส่วนบุคคลจะเก็บรวบรวมก่อน หรือหลัง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จะมีผลใช้บังคับทั้งฉบับ เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิในฐานะเจ้าของข้อมูลส่วนบุคคลข้างต้นทั้งสิ้น

7) หน้าที่ตรวจสอบความเป็นปัจจุบัน ความถูกต้อง และความสมบูรณ์ของข้อมูลส่วนบุคคล²⁸

ตามหลักในเรื่องความถูกต้อง สมบูรณ์ และเป็นปัจจุบันของข้อมูลส่วนบุคคล (Accuracy Principle) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการให้ข้อมูลส่วนบุคคลที่ตนประมวลผลหรือเก็บรักษาอยู่นั้นให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

8) หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม²⁹

ตามหลักในเรื่องการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Principle) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ออกประกาศ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งมีผลบังคับใช้เมื่อวันที่ 21 มิถุนายน พ.ศ. 2565 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการดังนี้

(1) ต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคล ดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์หรือรูปแบบอื่นใดก็ตาม

(2) ต้องประกอบด้วยมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (Physical Measures) ที่

²⁷ มาตรา 73 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²⁸ มาตรา 35 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

²⁹ มาตรา 37(1) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(3) ต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(4) ต้องคำนึงถึงความสามารถในการดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(5) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่างๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Servers) เครื่องคอมพิวเตอร์ลูกข่าย (Clients) และอุปกรณ์ต่างๆ ที่ใช้ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple Layers of Security Controls) เพื่อลดความเสี่ยงในกรณีที่มีมาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

(6) ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้ที่เหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งาน ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ประกอบกัน

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (Access Control) ที่มีการพิสูจน์ และยืนยันตัวตน (Identity Proofing and

Authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (Authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know Basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (User Registration and De-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of Privileged Access Rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบ ทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit Trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(จ) ต้องสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

บุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ
ประกอบกัน

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคล ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ในกรณีที่มีการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูล ส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำข้างต้น โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคล จะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ ด้วย

9) หน้าที่ป้องกันไม่ให้บุคคลที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย³⁰

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการที่เหมาะสมเมื่อต้องให้ข้อมูลแก่บุคคลหรือนิติบุคคลอื่น ที่ไม่ใช่ผู้ควบคุมข้อมูลเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

10) หน้าที่จัดให้มีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคล³¹

ตามหลักความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคล (Storage Limitation Principle) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคล ได้ถอนความยินยอม เว้นแต่กรณีที่ได้รับการยกเว้นตามกฎหมาย

11) หน้าที่แจ้งเหตุละเมิดข้อมูลส่วนบุคคล³²

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ออกประกาศ เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งมีผลบังคับใช้นับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป (วันที่ 15 ธันวาคม พ.ศ. 2565) โปรดดูรายละเอียดในบทที่ 8 แนวทางการปฏิบัติกรณีเกิดละเมิดข้อมูลส่วนบุคคล

³⁰ มาตรา 37(2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³¹ มาตรา 37(3) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³² มาตรา 37(4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

12) หน้าที่แต่งตั้งตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร³³

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แต่งตั้งตัวแทนในราชอาณาจักร ในกรณีที่

(ก) ผู้ควบคุมข้อมูลอยู่นอกราชอาณาจักร และ

(ข) ได้เสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร หรือเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

การแต่งตั้งตัวแทนนี้ต้องทำเป็นหนังสือและตัวแทนต้องไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

13) หน้าที่บันทึกการประมวลผลข้อมูลส่วนบุคคล³⁴

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการบันทึกการประมวลผลข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษรหรือระบบอิเล็กทรอนิกส์ โดยต้องมีรายการตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนดดังนี้

(ก) รายละเอียดของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(ข) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(ค) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(ง) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(จ) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล คุณสมบัติของบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(ฉ) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลกรณีผู้ควบคุมข้อมูลใช้หรือเปิดเผยข้อมูลที่ไม่ต้องได้รับความยินยอม

(ช) คำอธิบายและรายละเอียดกรณีการปฏิเสธคำขอในเรื่องเกี่ยวกับการขอสำเนาข้อมูลส่วนบุคคล หรือการส่งหรือโอนข้อมูลส่วนบุคคล หรือการคัดค้านการประมวลผล

³³ มาตรา 37(5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³⁴ มาตรา 39 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลของเจ้าของข้อมูล หรือการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง และเป็นปัจจุบัน

(ข) รายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

14) หน้าที่จัดให้มีข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)³⁵

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคล และมอบหมายหรือกำหนดให้บุคคลอื่นประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) กับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

15) หน้าที่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)³⁶

ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลเป็นไปตามหลักเกณฑ์เรื่องการตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการกำหนด ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอรวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (โปรดดูรายละเอียดใน *บทที่ 9 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล*)

3.2 ผู้ประมวลผลข้อมูลส่วนบุคคล

3.2.1 ความหมายของผู้ประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

จากคำนิยามข้างต้น ทั้งบุคคลธรรมดาและนิติบุคคลสามารถมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลได้เช่นกัน หากบุคคลธรรมดาหรือนิติบุคคลนั้น ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

³⁵ มาตรา 40 วรรค 3 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³⁶ มาตรา 41 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้จากคำนิยามที่ระบุว่า “...บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล...” ทำให้พิจารณาได้ว่า หากบุคคลใดมีลักษณะการดำเนินการเป็นผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว บุคคลนั้นก็จะไม่มีลักษณะและฐานะของผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ หากบุคคลหรือบริษัทใดเปลี่ยนจากการประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของบุคคลอื่นเป็นการประมวลผลข้อมูลส่วนบุคคลโดยการตัดสินใจของตนเอง บุคคลนั้นหรือบริษัทนั้นจะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคล และไม่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลทันที

3.2.2 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

1) หน้าที่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล³⁷

ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

หากผู้ประมวลผลข้อมูลส่วนบุคคลไม่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือข้อกำหนดในสัญญากับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะกลายเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมนั้น ๆ และจะทำให้มีหน้าที่และความรับผิดชอบตามกฎหมายเช่นเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล

2) หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และแจ้งเหตุละเมิด³⁸

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยมิชอบ รวมถึงแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

3) หน้าที่จัดทำและเก็บรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคล³⁹

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดทำและเก็บรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคลตามรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

³⁷ มาตรา 40 (1) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³⁸ มาตรา 40 (2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

³⁹ มาตรา 40 (3) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ออกประกาศ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 โดยมีผลบังคับใช้เมื่อวันที่ 17 ธันวาคม พ.ศ. 2565

4) หน้าที่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)⁴⁰

เช่นเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล หากลักษณะการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลเป็นไปตามที่คณะกรรมการกำหนด ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอรวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3.3 ตัวอย่างการพิจารณาผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

ตัวอย่างที่ 1

ในการเสนอขายผลิตภัณฑ์ประกันภัย บริษัท เอ ออกแบบผลิตภัณฑ์ประกันภัยอุบัติเหตุการเดินทางสำหรับผู้เดินทางจากประเทศไทยไปประเทศจีนโดยบริษัท เอ เป็นผู้กำหนดว่ากลุ่มลูกค้าเป้าหมายสำหรับผลิตภัณฑ์ประกันภัยนี้คือใคร และกำหนดประเภทข้อมูลส่วนบุคคลที่บริษัท เอจะต้องประมวลผลเพื่อที่จะพิจารณารับประกันภัย รวมถึงให้บริการต่าง ๆ แก่ลูกค้า (เจ้าของข้อมูลส่วนบุคคล) เมื่อบริษัท เอ จะเสนอขายผลิตภัณฑ์ให้กับกลุ่มลูกค้าเป้าหมาย บริษัท เอ จึงบอกกล่าวและมอบหมายให้ตัวแทนประกันวินาศภัยของตนดำเนินการเสนอขายให้แก่ลูกค้า นอกจากนั้น บริษัท เอ ยังส่งข้อมูลจำพวก ชื่อ-นามสกุล หมายเลขโทรศัพท์ และที่อยู่ของลูกค้าให้กับผู้รับจ้างพิมพ์และส่งกรมธรรม์ประกันภัยให้แก่ลูกค้า

ในกรณีนี้

1. บริษัท เอ – เป็นผู้ตัดสินใจในการเลือกประเภทเจ้าของข้อมูลส่วนบุคคล ประเภทข้อมูลส่วนบุคคลที่จะจัดเก็บ และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ดังนั้น บริษัท เอ จึงประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล
2. ตัวแทนประกันภัยของบริษัท เอ - ดำเนินการเสนอขายผลิตภัณฑ์ประกันภัยอุบัติเหตุการเดินทางตามคำสั่ง และในนามของบริษัท เอ ดังนั้น ตัวแทนประกันวินาศภัยจึงประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

⁴⁰ มาตรา 41 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3. บริษัทรับจ้างพิมพ์และส่งกรมธรรม์ประกันภัย – ประมวลผลข้อมูลส่วนบุคคลที่ได้รับมาจากบริษัท เอ เพื่อดำเนินการพิมพ์และจัดส่งกรมธรรม์ประกันภัยตามคำสั่งของบริษัท เอ ดังนั้นบริษัทรับจ้างพิมพ์และส่งกรมธรรม์ประกันภัยจึงประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อสังเกต

แม้ตัวแทนประกันวินาศภัย จะมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ของบริษัทประกันภัย แต่หากตัวแทนประกันวินาศภัยกระทำการใด ๆ เกี่ยวกับการเก็บ ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลที่นอกเหนือไปจากคำสั่งของบริษัทประกันภัย หรือเพื่อประโยชน์ของตัวแทนประกันภัยเองเป็นการเฉพาะตัวแทนประกันวินาศภัยจะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลโดยอัตโนมัติ ซึ่งสำหรับการกระทำดังกล่าว จะไม่อยู่ในขอบเขตความรับผิดชอบของบริษัทประกันภัย และตัวแทนประกันวินาศภัยจะต้องรับผิดชอบและมีความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากบริษัทประกันภัยในการดำเนินการนอกเหนือคำสั่งดังกล่าว

ตัวอย่างที่ 2

บริษัท เอ เก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่ซื้อประกันภัยสุขภาพมาและดำเนินการเข้าทำสัญญารับประกันภัยต่อกับผู้รับประกันภัยต่อในต่างประเทศ โดยบริษัทรับประกันภัยต่อนำข้อมูลที่ได้จากบริษัท เอ มาประมวลผลเพื่อพิจารณารับประกันภัยต่อให้กับบริษัท เอ

กรณีนี้

1. บริษัท เอ – ประมวลผลข้อมูลส่วนบุคคลของลูกค้าที่ซื้อประกันภัยสุขภาพเพื่อพิจารณารับประกันภัยและให้บริการต่าง ๆ ตามสัญญาประกันภัย รวมถึงการนำข้อมูลมาตัดสินใจเกี่ยวกับการเข้าทำสัญญารับประกันภัยต่อ ดังนั้น บริษัท เอ จึงประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล
2. บริษัทรับประกันภัยต่อ – นำข้อมูลส่วนบุคคลของลูกค้าที่ได้จากบริษัท เอ มาประมวลผลเพื่อพิจารณารับประกันภัยต่อเพื่อเข้าทำสัญญากับบริษัท เอ โดยบริษัทรับประกันภัยต่อมีอำนาจตัดสินใจว่าจะนำข้อมูลใดมาพิจารณาในการรับประกันภัยต่อ ดังนั้นบริษัทรับประกันภัยต่อจึงเป็นผู้ควบคุมข้อมูลส่วนบุคคล (ไม่ใช่ผู้ประมวลผลของบริษัท เอ)

ตัวอย่างที่ 3

บริษัท เอ รับประกันภัยรถยนต์ของนาย ก. ต่อมานาย ก. เกิดอุบัติเหตุทางรถยนต์จึงแจ้งบริษัท เอ เพื่อให้บริษัท เอ ดำเนินการให้บริการเกี่ยวกับการเรียกค่าสินไหมทดแทน เมื่อบริษัท เอ ได้รับการแจ้งจากนาย ก. แล้ว บริษัท เอ จึงแจ้งนายหนึ่ง ซึ่งเป็นผู้ให้บริการสำรวจความเสียหายของรถยนต์ พร้อมทั้งให้ข้อมูลชื่อ -

นามสกุล เลขทะเบียนรถยนต์ และหมายเลขโทรศัพท์ของนาย ก. เพื่อให้นายหนึ่งเข้าดำเนินการตรวจสอบความเสียหายและให้บริการแก่นาย ก.

ในกรณีนี้

1. บริษัท เอ – ประมวลผลข้อมูลส่วนบุคคลของนาย ก. เพื่อการรับประกันภัย และการให้บริการต่าง ๆ รวมถึงการจ่ายค่าสินไหมทดแทนแก่นาย ก. โดยบริษัท เอ มีอำนาจตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของนาย ก. ในทุกขั้นตอน ดังนั้น บริษัท เอ จึงประมวลผลข้อมูลส่วนบุคคลของนาย ก. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

2. นายหนึ่ง – รับข้อมูลส่วนบุคคลของนาย ก. ได้แก่ ชื่อ-นามสกุล เลขทะเบียนรถยนต์ และหมายเลขโทรศัพท์ของนาย ก. มาจากบริษัท เอ เพื่อดำเนินการประเมินความเสียหายและให้บริการแก่นาย ก. ตามคำสั่งของบริษัท เอ ดังนั้น นายหนึ่ง จึงประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อสังเกต

- ในเรื่องความสัมพันธ์ระหว่างบริษัทและนายหน้าประกันวินาศภัยนั้น โดยทั่วไปมักเป็นความสัมพันธ์ที่ต่างฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคลด้วยตนเอง แต่ทั้งนี้ ในการกำหนดหรือระบุสถานะของคู่ค้า หรือระหว่างบริษัทกับนายหน้าประกันวินาศภัยนั้น ยังจำต้องขึ้นอยู่กับลักษณะการดำเนินการตามแต่ละกรณี
- ในความสัมพันธ์ระหว่างบริษัทและบริษัทรับประกันภัยต่อ เพื่อวัตถุประสงค์ในการรับประกันภัยต่อจากบริษัท และบริษัทรับประกันภัยต่อต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคลทั้งสองฝ่าย เนื่องจากทั้งสองบริษัทต่างมีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลในส่วนของตนเอง กล่าวคือ บริษัทมีอำนาจตัดสินใจว่าจะนำข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประกันภัยใดบ้างเพื่อนำไปรับประกันภัยต่อ และบริษัทรับประกันภัยต่อเองก็มีอำนาจในการกำหนดประเภทข้อมูลส่วนบุคคลที่จะใช้ในการพิจารณารับประกันภัยต่อเช่นกัน
- การพิจารณาความสัมพันธ์ระหว่างคู่ค้า หรือคู่สัญญาของบริษัท ว่าคู่ค้า และบริษัทเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคลนั้นล้วนขึ้นอยู่กับลักษณะการดำเนินธุรกิจ และลักษณะความสัมพันธ์ในแต่ละกรณีไป ดังนั้น บริษัทควรจรรवरวบรวมรายชื่อคู่ค้าและคู่สัญญาของบริษัททั้งหมดมาเพื่อพิจารณาความสัมพันธ์และบทบาทของบริษัทและคู่สัญญาของบริษัท เพื่อที่ทั้งคู่จะได้ทราบถึงสิทธิและหน้าที่ของตนเองในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้อย่างถูกต้อง

บทที่ 4 แนวทางการแยกประเภทข้อมูลส่วนบุคคล

4.1 ขอบเขตและประเภทข้อมูลส่วนบุคคล

ขั้นตอนแรกในการดำเนินการเพื่อปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล คือ การระบุและแยกประเภทว่าข้อมูลใดบ้างเป็นข้อมูลส่วนบุคคล และข้อมูลใดบ้างที่ไม่เป็นข้อมูลส่วนบุคคล เนื่องจากการประมวลผลข้อมูลที่อยู่ในความหมายของคำว่า “ข้อมูลส่วนบุคคล” จะต้องดำเนินการตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนด แต่ในทางกลับกันข้อมูลใดที่ไม่มีลักษณะเป็น “ข้อมูลส่วนบุคคล” การดำเนินการกับข้อมูลดังกล่าวไม่จำเป็นต้องดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

4.1.1 หลักเกณฑ์การพิจารณาข้อมูลส่วนบุคคล

ตามที่ได้ระบุในบทที่ 1 ขอบเขตการใช้บังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล การพิจารณาเพื่อแยกประเภทข้อมูลส่วนบุคคลต้องพิจารณาจากความหมายของคำว่า “ข้อมูลส่วนบุคคล” ดังนี้

โดยทั่วไป “ข้อมูล” มีความหมาย “ข้อเท็จจริง หรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ”

ข้อสังเกต

“ข้อเท็จจริง” มีความหมายว่า ข้อความหรือเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่ตามจริง เรื่องหรือประเด็นที่เกี่ยวกับเหตุการณ์ พฤติกรรม หรือสิ่งใด ๆ ที่เกิดขึ้น ที่มีอยู่ หรือที่เป็นไป

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ⁴¹

“บุคคล” หมายความว่า บุคคลธรรมดา⁴²

จากความหมายข้างต้น สรุปได้ว่า “ข้อมูลส่วนบุคคล” คือ ข้อมูลที่มีลักษณะดังต่อไปนี้

- 1) เป็นข้อมูลของบุคคลธรรมดา
- 2) เจ้าของข้อมูลส่วนบุคคลยังไม่ถึงแก่ความตาย

⁴¹ มาตรา 6 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

⁴² มาตรา 6 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3) ข้อมูลนั้นสามารถระบุตัวบุคคลได้ไม่ว่าทางตรง หรือทางอ้อม

ข้อพึงระวัง

ในการพิจารณาว่าข้อมูลใดสามารถระบุไปถึงตัวบุคคลได้หรือไม่นั้น มีข้อพึงระวังว่า ข้อมูลบางอย่างที่บริษัทเก็บรวบรวมอยู่หรือจะเก็บรวบรวมนั้น แม้จะไม่สามารถระบุตัวบุคคลได้โดยตรง แต่ข้อมูลนั้นอาจจะระบุตัวบุคคลได้ในทางอ้อม ซึ่งหากเป็นเช่นนั้น ข้อมูลดังกล่าวจะถือว่าเป็นข้อมูลส่วนบุคคลภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เช่น วันเดือนปีเกิด ศาสนา อายุ เพศ ทะเบียนรถยนต์ เป็นต้น

นอกจากนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยังได้กำหนดประเภทข้อมูลส่วนบุคคลบางประเภทที่มีฐานประมวลผลโดยชอบด้วยกฎหมายแตกต่างไปจากฐานการประมวลผลโดยชอบด้วยกฎหมายของข้อมูลส่วนบุคคลทั่วไป เนื่องจาก การประมวลผลข้อมูลส่วนบุคคลเหล่านั้นอาจทำให้เกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคลได้ง่าย หรืออาจทำให้เกิดผลกระทบที่ร้ายแรง สร้างความขัดแย้งได้ง่าย โดยประเภทของข้อมูลส่วนบุคคลเหล่านั้นถูกกำหนดอยู่ในมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจเรียกข้อมูลส่วนบุคคลเหล่านั้นว่า เป็น “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หรือ Sensitive Personal Data ดังนี้

1. ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ หรือเผ่าพันธุ์
2. ข้อมูลส่วนบุคคลเกี่ยวกับความเห็นทางการเมือง
3. ข้อมูลส่วนบุคคลเกี่ยวกับความเชื่อในลัทธิ ศาสนาหรือปรัชญา
4. ข้อมูลส่วนบุคคลเกี่ยวกับความพิการ
5. ข้อมูลส่วนบุคคลเกี่ยวกับพฤติกรรมทางเพศ
6. ข้อมูลสหภาพแรงงาน
7. ข้อมูลสุขภาพ
8. ข้อมูลพันธุกรรม
9. ข้อมูลชีวภาพ
10. ประวัติอาชญากรรม
11. ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการกำหนด

ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยังได้อธิบายความหมายของ “ข้อมูลชีวภาพ” เพิ่มเติมไว้ว่า หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวกับการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้แยกแยะและยืนยันตัวบุคคลของบุคคลนั้นที่ไม่เหมือนบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ เป็นต้น

ข้อพึงระวัง

แม้ว่าข้อมูลทางการเงินจะยังไม่ได้ถูกจัดอยู่ในประเภทข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แต่การประมวลผลข้อมูลทางการเงินควรต้องใช้ความระมัดระวังมากเป็นพิเศษ เนื่องจากข้อมูลดังกล่าวมีความอ่อนไหวสูง กล่าวคือ อาจทำให้เกิดผลกระทบกับผู้ควบคุมข้อมูลส่วนบุคคลได้มาก และการพิสูจน์ความเสียหายสามารถทำได้ง่าย เช่น การนำตัวเลขในข้อมูลทางการเงินไปพิสูจน์เรียกค่าสินไหมทดแทน เป็นต้น

4.1.2 การพิจารณาเจ้าของข้อมูลส่วนบุคคล

แม้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจะไม่ได้กำหนดความหมายของ “เจ้าของข้อมูลส่วนบุคคล” ไว้ แต่หากพิจารณาจากความหมายของคำว่า “ข้อมูลส่วนบุคคล” และ “บุคคล” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลแล้ว สามารถพิจารณาได้ว่า “เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดาที่ยังมีชีวิตอยู่ที่ถูกระบุหรือสามารถระบุตัวได้ด้วยข้อมูลที่เกี่ยวข้องกับบุคคลนั้น

ข้อสังเกต

ข้อมูลหนึ่งชุดอาจเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลได้หลายคน เนื่องจากเป็นข้อมูลที่สามารถระบุตัวบุคคลได้หลายคน เช่น สำเนาทะเบียนบ้านซึ่งประกอบด้วยชื่อเจ้าบ้านและบุคคลที่อาศัยอยู่ในบ้าน ซึ่งอาจเป็นคนละคนกัน เช่น ชื่อเจ้าบ้าน คือ นาย ก. มีผู้อาศัยตามทะเบียนบ้านคือ นาง ข. กับ นางสาว ค. ดังนั้น สำเนาทะเบียนบ้านเล่มดังกล่าวอาจระบุได้ถึงตัวบุคคลทั้ง นาย ก. นาง ข. และนางสาว ค.

4.1.3 ข้อมูลของผู้มีฐานะ/ข้อมูลของผู้เสียชีวิต

เนื่องจากข้อมูลของผู้เสียชีวิตไม่ได้ถือว่าเป็นข้อมูลที่ได้รับคุ้มครองตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ดังนั้น การประมวลผลเกี่ยวกับข้อมูลของผู้เสียชีวิตจึงไม่ต้องดำเนินการตามข้อกำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

การพิจารณาว่าข้อมูลใดเป็นข้อมูลของผู้เสียชีวิต อาจพิจารณาได้จากเวลาที่บุคคลเสียชีวิต กล่าวคือ เจ้าของข้อมูลส่วนบุคคลเสียชีวิตเมื่อใด ข้อมูลของบุคคลนั้นทั้งหมดย่อมไม่ใช่ “ข้อมูลส่วนบุคคล” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเมื่อนั้น (ไม่ว่าจะเก็บรวบรวมก่อน หรือหลังจากที่บุคคลถึงแก่ความตาย) ทั้งนี้ หาก

ขณะที่บริษัทเก็บรวบรวมข้อมูลเจ้าของข้อมูลได้ถึงแก่ความตายแล้ว ข้อมูลที่บริษัทเก็บรวบรวมจะไม่ถือเป็นข้อมูลส่วนบุคคลตั้งแต่แรก ณ ขณะที่บริษัทเก็บรวบรวม

ข้อพึงระวัง

แม้ว่าข้อมูลของผู้เสียชีวิตจะไม่ได้ได้รับความคุ้มครองตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แต่การประมวลผลข้อมูลส่วนบุคคลของผู้เสียชีวิตอาจอยู่ภายใต้กฎหมายฉบับอื่นได้ เช่น ประมวลกฎหมายอาญา ฐานหมิ่นประมาท เป็นต้น

4.2 แนวทางการแยกประเภทข้อมูลส่วนบุคคล

เมื่อกำหนดและระบุได้แล้วว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทก็จะสามารถนำข้อมูลเหล่านั้นมาพิจารณาแยกประเภทของข้อมูลส่วนบุคคลเพื่อการบริหารจัดการข้อมูลส่วนบุคคลของบริษัทได้ โดยลักษณะและวิธีการแยกประเภทข้อมูลส่วนบุคคล อาจดำเนินการได้ดังนี้

4.2.1 การพิจารณาความสามารถในการระบุไปถึงเจ้าของข้อมูล

หนึ่งในลักษณะของการเป็นข้อมูลส่วนบุคคล คือ ข้อมูลนั้น ๆ ต้องระบุไปถึงตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม ดังนั้น บริษัทจึงต้องพิจารณาด้วยว่าข้อมูลที่บริษัทเก็บรวบรวม หรือจะเก็บรวบรวมมีลักษณะหรือความเป็นไปได้ที่จะสามารถระบุตัวบุคคลบุคคลหนึ่งได้หรือไม่ โดยการพิจารณาความสามารถในการระบุตัวบุคคลของข้อมูลสามารถพิจารณาได้ ดังนี้

1) **ลักษณะการแยกแยะ (Distinguishability)** หมายถึง ข้อมูลที่มีลักษณะที่สามารถแยกแยะตัวบุคคลได้ เช่น ชื่อ-นามสกุล หรือเลขบัตรประจำตัวประชาชน หรือเลขกรมธรรม์ประกันภัยสุขภาพ ข้อมูลทางชีวภาพต่าง ๆ เช่น ม่านตา ลายนิ้วมือ ข้อมูลอัตลักษณ์เสียง ภาพใบหน้าที่ใช้เทคโนโลยีจดจำใบหน้า (Face Recognition) เป็นต้น

2) **ลักษณะการติดตาม (Traceability)** หมายถึง ข้อมูลที่มีลักษณะที่สามารถใช้ติดตามตัวบุคคลได้ เช่น พฤติกรรมการใช้งานเว็บไซต์ หรือ Log File เป็นต้น

3) **ลักษณะการเชื่อมโยง (Likability)** หมายถึง ข้อมูลที่มีลักษณะที่สามารถเชื่อมโยง หรืออาจเชื่อมโยงกันเพื่อระบุตัวบุคคลได้ เช่น ข้อมูลสองชุดที่แยกจากกัน แต่หากรวมเข้าด้วยกันแล้วก็จะสามารถระบุตัวบุคคลได้ เช่น ทะเบียนรถยนต์ เลขประจำตัวผู้พลาย เพศ อายุ เป็นต้น

ตัวอย่างข้อมูลที่มีลักษณะการเชื่อมโยง

บริษัท เอ เก็บรวบรวมหมายเลขทะเบียนรถยนต์ของผู้เอาประกันภัยทุกรายของบริษัทไว้ในถังข้อมูลหนึ่ง และเก็บรายละเอียดอื่น ๆ ของผู้เอาประกันภัย เช่น ชื่อ-นามสกุล เลขบัตรประจำตัวประชาชน ของผู้เอาประกันภัยไว้ในถังข้อมูลที่สอง กรณีนี้ เมื่อข้อมูลเลขทะเบียนรถยนต์แยกกับข้อมูลอื่น ๆ บริษัทจะไม่สามารถทราบถึงตัวบุคคลผู้เป็นเจ้าของทะเบียนรถยนต์ดังกล่าวได้ แต่หากบริษัทนำข้อมูลทะเบียนรถยนต์ที่อยู่ในถังข้อมูลทั้งสองมารวบรวมกัน จะทำให้บริษัทระบุตัวเจ้าของเลขทะเบียนรถยนต์นั้นได้ เช่นนี้เลขทะเบียนรถยนต์เป็นข้อมูลที่มีลักษณะการเชื่อมโยงตัวบุคคลได้

หากข้อมูลที่บริษัทจัดเก็บ หรือจะจัดเก็บมีลักษณะอย่างหนึ่งอย่างใดข้างต้น ข้อมูลนั้นจะถือว่าเป็นข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

4.2.2 การพิจารณากำหนดชั้นความลับของข้อมูลส่วนบุคคล

การพิจารณากำหนดชั้นความลับของข้อมูลส่วนบุคคลเพื่อกำหนดมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอาจพิจารณาได้จากกรณีดังต่อไปนี้

1) การกำหนดปัจจัยในการแยกประเภทข้อมูล

ปัจจัยที่อาจนำมาใช้ในการพิจารณากำหนดชั้นความลับเพื่อจัดทำมาตรการในการรักษาความปลอดภัยของข้อมูล อาจพิจารณาได้หลายปัจจัย เช่น ระดับความลับของข้อมูล (Confidentiality) ระดับความอ่อนไหวของข้อมูล (Sensitivity) หรือระดับการเชื่อมโยงตัวบุคคล (Likability)

ตัวอย่าง

ข้อมูลที่เปิดเผยหรืออาจพบได้ในสาธารณะ เช่น ชื่อ-นามสกุล ชื่อ Facebook ถือว่าเป็นข้อมูลที่มีความน่าเชื่อถือต่ำ การรักษาความปลอดภัยของข้อมูลเหล่านี้อาจกำหนดให้อยู่ในระดับเบื้องต้นได้ หรือข้อมูลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) เป็นข้อมูลที่มีความอ่อนไหวสูง อาจกำหนดให้มีมาตรการรักษาความปลอดภัยระดับสูงมาก เป็นต้น

2) การพิจารณาความเสี่ยงหากเกิดการละเมิดข้อมูลส่วนบุคคล

เมื่อบริษัทพิจารณากำหนดปัจจัยในการกำหนดชั้นความลับของข้อมูลส่วนบุคคลแล้ว บริษัทอาจพิจารณาประกอบกับความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลเหล่านั้นเกิดการรั่วไหลหรือเกิดการละเมิด เช่น ความเสี่ยงต่อชื่อเสียง ความเสี่ยงทางกฎหมาย (เช่น บทลงโทษ) หรือความเสี่ยงทางการเงิน เป็นต้น

4.2.3 ข้อมูลที่ทำให้ไม่สามารถระบุตัวบุคคลได้ (De-Identified Data)

ข้อมูลที่ทำให้ไม่สามารถระบุตัวบุคคลได้ หมายถึงข้อมูลที่มีการนำข้อมูลที่สามารถใช้ในการระบุตัวบุคคลได้โดยตรง (Direct Identifiers) เช่น ชื่อ – นามสกุล ออกจากชุดข้อมูลที่เก็บรวบรวมอย่างถาวรในลักษณะที่ไม่สามารถทำให้ข้อมูลเหล่านั้นกลับมาระบุตัวบุคคลได้อีก ซึ่งข้อมูลที่ไม่สามารถระบุตัวบุคคลได้นั้น จะไม่เป็นข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และการประมวลผลข้อมูลส่วนบุคคลดังกล่าว ก็ไม่ต้องดำเนินการตามข้อกำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

เช่น บริษัท เอ เก็บรวบรวมข้อมูลของนายหนึ่ง ผู้เอาประกันภัยไว้ ได้แก่ ชื่อ-นามสกุล หมายเลขโทรศัพท์ เลขบัตรประจำตัวประชาชน เพศ อายุ ที่อยู่ จำนวนเบี้ยประกันภัย จำนวนเงินเอาประกัน วันที่ซื้อประกันภัย เลขกรมธรรม์ (ชุดข้อมูล ก.) ต่อมากรมธรรม์ประกันภัยของนายหนึ่ง ผู้เอาประกันภัยได้สิ้นสุดลง และนายหนึ่งไม่ได้ซื้อประกันของ บริษัท เอ มาเป็นระยะเวลา 5 ปีแล้ว แต่บริษัท เอ อยากเก็บข้อมูลการซื้อกรมธรรม์ประกันภัยของนายหนึ่งเอาไว้เป็นสถิติของบริษัท บริษัท เอ จึงดำเนินการนำข้อมูลที่เป็น ชื่อ-นามสกุล เลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ เลขที่กรมธรรม์ประกันภัย ออกจากชุดข้อมูลของนายหนึ่ง อันทำให้ชุดข้อมูลของนายหนึ่งเหลือเพียงข้อมูล เพศ อายุ ที่อยู่ เบี้ยประกันภัย และวันที่ซื้อประกันภัย (ชุดข้อมูล ข.) ซึ่งข้อมูลดังกล่าวไม่อาจจะกลับไปได้ว่าเป็นข้อมูลของนายหนึ่ง ดังนั้น ชุดข้อมูล ข. จึงไม่ใช่ข้อมูลส่วนบุคคล การประมวลผลชุดข้อมูล ข. จึงไม่ต้องดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

4.2.4 ข้อมูลนิรนาม (Anonymized Data)

ข้อมูลนิรนาม (Anonymized Data) หมายถึง ข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้ยาก หรือทำให้ไม่สามารถระบุตัวบุคคลได้เพียงชั่วคราว

การที่ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนามนั้น ไม่ได้ทำให้ข้อมูลดังกล่าวไม่เป็นข้อมูลส่วนบุคคลอีกต่อไป แต่การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนามเป็นวิธีการหนึ่งในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลซึ่งมีการใช้วิธีการนี้กันอย่างแพร่หลายในระดับสากล เนื่องจากการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนามนั้นสามารถลดความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่ถูกควบคุมข้อมูลส่วนบุคคลเก็บรักษาอยู่ได้ เนื่องจากข้อมูลเหล่านั้นยากที่จะระบุตัวบุคคลได้ (แต่ยังคงสามารถทำให้ระบุตัวบุคคลได้)

ข้อแตกต่างที่สำคัญของการทำให้ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (De-Identified Data) และข้อมูลนิรนาม (Anonymized Data) คือ ข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (De-Identified Data) นั้นไม่สามารถเชื่อมโยงหรือระบุตัวบุคคลได้อย่างถาวร อันทำให้ไม่เป็นข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แต่ข้อมูลนิรนามยังอาจจะระบุตัวบุคคลได้ ซึ่งยังคงถือเป็นข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

4.2.5 การแฝงข้อมูล (Pseudonymization)

การแฝงข้อมูล เป็นวิธีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลวิธีหนึ่งซึ่งเป็นการนำชุดข้อมูลส่วนบุคคลมาเปลี่ยนเป็นเลข หรือรหัส ที่สามารถอ่านเป็นข้อมูลส่วนบุคคลชุดเดิมได้ โดยประโยชน์ของการแฝงข้อมูลส่วนบุคคลนี้คือสามารถลดความเสี่ยงในการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคลได้ กล่าวคือ หากผู้ได้รับข้อมูลแฝงจากการละเมิด หรือการรั่วไหลของข้อมูลไม่มีระบบ หรือเทคนิคในการทำให้ข้อมูลแฝงกลับมาเป็นข้อมูลที่ระบุตัวบุคคลได้ ความเสี่ยงและความเสียหายจากการละเมิดข้อมูลส่วนบุคคลจะลดลง

ทั้งนี้ เนื่องจากข้อมูลที่ถูกแฝงนั้นยังคงสามารถระบุตัวบุคคลได้ เพียงแต่ถูกแฝงด้วยรหัสหรือตัวเลข ดังนั้น ข้อมูลที่ถูกแฝงยังคงเป็นข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อยู่ การประมวลผลข้อมูลส่วนบุคคลแฝงจึงยังต้องดำเนินการตามข้อกำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

บทที่ 5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผย (รวมเรียกว่า “การประมวลผล”) ข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จำเป็นต้องมีฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย (Lawful Basis) เพราะการประมวลผลข้อมูลส่วนบุคคลของบุคคลย่อมเป็นการนำข้อมูลส่วนบุคคลมาใช้ประโยชน์ ซึ่งไม่อาจกระทำได้เว้นแต่มีกฎหมายอนุญาตให้ทำได้ ดังนั้น ในการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องกระทำไปโดยอาศัยอำนาจตามกฎหมายไม่ว่าในกรณีใด ๆ กล่าวคือ ฐานในการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย หรือฐานโดยชอบด้วยกฎหมาย

ดังนั้น การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีฐานโดยชอบด้วยกฎหมาย (Lawful Basis) จึงเป็นความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยทันที ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดฐานโดยชอบด้วยกฎหมาย (Lawful Basis) สำหรับข้อมูลส่วนบุคคลสองประเภทดังที่ได้อธิบายไปแล้วข้างต้น กล่าวคือ

ฐานในการประมวลผลข้อมูลส่วนบุคคลทั่วไป ซึ่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้รับเอาหลักการส่วนใหญ่มาจากหลักการของ GDPR โดยสามารถแบ่งออกเป็นฐานโดยชอบด้วยกฎหมาย ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลทั่วไป ได้ดังต่อไปนี้

- ฐานความยินยอม (Consent)
- ฐานสัญญา (Contractual Necessity)
- ฐานประโยชน์ที่สำคัญต่อชีวิต (ระงับอันตรายต่อชีวิต ร่างกาย สุขภาพ) (Vital Interest)
- ฐานหน้าที่ตามกฎหมาย (Legal Obligation)
- ฐานภารกิจของรัฐ (Public Task)
- ฐานประโยชน์อันชอบธรรม (Legitimate Interest)
- ฐานจดหมายเหตุ/ วิจัย/ สถิติ (หมายเหตุ: ไม่มีกำหนดเป็นการเฉพาะตามหลักการของ GDPR)

ฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) จะแตกต่างจากฐานในการประมวลผลข้อมูลส่วนบุคคลทั่วไปข้างต้น โดยฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวมีดังนี้

- ฐานความยินยอมโดยชัดแจ้ง (Explicit Consent)
- ฐานประโยชน์ที่สำคัญต่อชีวิต (Vital Interest)
- ฐานเพื่อการดำเนินการของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร (Not-for-Profit Body)
- ฐานข้อมูลที่เปิดเผยโดยสาธารณะโดยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (หมายเหตุ: หลักการคล้ายคลึงกับ GDPR แต่ถ้อยคำสามารถพิจารณาตีความได้แตกต่างกัน)
- ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับสิทธิเรียกร้อง (Legal Claims)
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคม (Employment, Social Security and Social Protection Law)
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับเวชศาสตร์ป้องกัน หรืออาชีวศาสตร์ (Health or Social Care)
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข (Public Health)
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ (Archiving, Research and Statistics)
- ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ (Substantial Public Interest)

ข้อสังเกต

ในการพิจารณาฐานโดยชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลส่วนบุคคลทั่วไปหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว บริษัทต้องพิจารณาจากวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลในแต่ละกิจกรรม เช่น บริษัทจะเปิดเผยชื่อ-นามสกุล ของผู้เอาประกันภัยต่อ ปปง. ตาม พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน เช่นนี้วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล (ชื่อ-สกุล ของผู้เอาประกันภัย) ของบริษัทในกิจกรรมการประมวลผลนี้คือ การปฏิบัติตามกฎหมายซึ่งเป็นหน้าที่ตามกฎหมายที่บริษัทต้องทำ ดังนั้น ฐานในการประมวลผลข้อมูลส่วนบุคคลในกรณีนี้คือฐานหน้าที่ตามกฎหมาย (Legal Obligation)

ดังนั้น จะสังเกตได้ว่า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดฐานโดยชอบด้วยกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลทั้งที่เป็นข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ไว้อย่างแตกต่างกัน ดังนั้น ในการประมวลผลข้อมูลส่วนบุคคลนั้น บริษัทจึงจำเป็นต้องระบุหรือแยกประเภทข้อมูลส่วนบุคคลก่อน จึงจะสามารถพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลได้อย่างถูกต้องตามกฎหมาย

รายละเอียดของฐานโดยชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคล มีดังต่อไปนี้

5.1 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป

ฐานในการประมวลผลข้อมูลส่วนบุคคลทั่วไป พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล รับหลักการส่วนใหญ่มาจาก GDPR ดังนั้น การตีความหรือแนวทางในการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลในแนวปฏิบัติฉบับนี้จึงเป็นไปตามหลักการของ GDPR

ตารางเปรียบเทียบระหว่างฐานโดยชอบด้วยกฎหมายที่กำหนดไว้ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกับ GDPR สำหรับการประมวลผลข้อมูลส่วนบุคคลทั่วไป

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	GDPR
ฐานความยินยอม	Consent
ฐานสัญญา	Contractual Necessity
ฐานประโยชน์ที่สำคัญต่อชีวิต	Vital Interest
ฐานหน้าที่ตามกฎหมาย	Legal Obligation
ฐานภารกิจของรัฐ	Public Task
ฐานประโยชน์อันชอบธรรม	Legitimate Interest
ฐานจดหมายเหตุ/ วิจัย/ สถิติ	ไม่มีการกำหนด ฐานจดหมายเหตุ/ วิจัย/ สถิติ

5.1.1 ฐานความยินยอม (Consent)

5.1.1.1 เงื่อนไขของการขอความยินยอม

มาตรา 19 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดเงื่อนไขของการขอความยินยอมไว้ ดังนี้

1) ความยินยอมจะต้องมีอยู่ก่อนหรือขณะที่จะมีการประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือ ขณะที่ จะทำการเก็บรวบรวมข้อมูลส่วนบุคคล

2) การขอความยินยอมต้องทำโดยชัดแจ้ง

ด้วยเหตุที่ว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยังไม่มีคำวินิจฉัยหรือแนวทางในการพิจารณาว่า การขอความยินยอมอย่างไรจึงจะถือว่าเป็นการขอความยินยอมโดยชัดแจ้ง ดังนั้น แนวทางปฏิบัติฉบับนี้ จึงนำแนวทางปรับใช้ GDPR⁴³ มาพิจารณาและขอเสนอแนะแนวทางที่ดีความ คำว่า “การขอความยินยอมโดยชัดแจ้ง” หมายถึง การขอความยินยอมโดยไม่คลุมเครือ (Unambiguous) เพื่อให้เจ้าของข้อมูลส่วนบุคคลกระทำการให้ความยินยอมที่ชัดเจน (Clear Affirmative Action) ซึ่งไม่ใช่การขอความยินยอมที่มีลักษณะที่ถือเอาการเงียบเฉย หรือการตกลงเลือกในช่องว่างหน้า (Pre-Tricked Box) หรือการไม่กระทำการ (Inactivity) เป็นการให้ความยินยอม ดังนั้น บริษัทควรจัดให้การให้ความยินยอมกระทำในลักษณะที่มีการกระทำ (Positive Action) เช่น การลงลายมือชื่อ หรือ การเลือกตกลงในช่องว่าง หรือการเลื่อนนิ้วมือไปบนหน้าจออุปกรณ์อิเล็กทรอนิกส์ตามตำแหน่งที่กำหนด (Swipe Bar) เป็นต้น เพื่อให้แน่ใจว่า บริษัทได้ปฏิบัติตามเงื่อนไขแล้ว

3) การขอความยินยอมต้องทำเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจทำได้

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้การขอความยินยอมที่ชัดแจ้งนั้นจะต้องกระทำเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ อย่างไรก็ตาม หากโดยสภาพแล้วไม่อาจขอความยินยอมเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ได้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยกเว้นให้การขอความยินยอมนั้นสามารถกระทำได้โดยวิธีอื่น เช่น การขอความยินยอมผ่านทางโทรศัพท์ (Telesales หรือ Telemarketing) เป็นต้น ซึ่งโดยสภาพไม่ควรถือว่าสามารถขอความยินยอมใน

⁴³ Information Commissioner's Office, UK (ICO), 'What is valid consent?', ICO <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#what1>> accessed 11 April 2020

รูปแบบของการทำหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ได้ บริษัทจึงอาจใช้การบันทึกเสียงในการขอความยินยอมใด ๆ จากลูกค้าแทนได้

4) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลต้องถูกระบุชัดเจน

ประเด็นที่สำคัญที่สุดอย่างหนึ่งในการประมวลผลข้อมูลส่วนบุคคล คือ วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เนื่องจากวัตถุประสงค์ดังกล่าวจะถูกนำไปเป็นข้อพิจารณาว่ากิจกรรมภายใต้วัตถุประสงค์ในการการประมวลผลนั้นตั้งอยู่บนฐานโดยชอบด้วยกฎหมายใด และส่งผลไปถึงขอบเขตในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวด้วย ดังนั้น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จึงกำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลรับทราบและเข้าใจว่า ข้อมูลส่วนบุคคลของตนจะถูกนำไปใช้ประโยชน์อย่างไรบ้าง

ทั้งนี้ หากวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่แตกต่างกันย่อมต้องใช้ความยินยอมแยกกัน⁴⁴ โดยวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่แจ้งไปนั้นจะต้องมีครอบคลุมไปถึงกิจกรรมนั้น ๆ ด้วย ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลควรตรวจสอบความครอบคลุมของความยินยอมอยู่เสมอว่ายังใช้ได้กับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่เปลี่ยนไปหรือไม่ หากวัตถุประสงค์ที่ได้แจ้งไว้แล้วเปลี่ยนไปจากขอบเขตความยินยอมที่ได้ขอไว้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีการขอความยินยอมสำหรับวัตถุประสงค์ใหม่ที่เปลี่ยนไปนั้น

อย่างไรก็ตามในการดำเนินธุรกิจประกันวินาศภัยส่วนใหญ่ บริษัทสามารถอ้างอิงตามฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่นนอกจากฐานความยินยอมเป็นหลัก (ความยินยอมจะต้องไม่ใช่ฐานที่บริษัทใช้เป็นหลักในการประกอบธุรกิจ) เช่น ฐานหน้าที่ตามกฎหมาย ฐานสัญญา เป็นต้น เหลือแต่เพียงบางวัตถุประสงค์ เช่น การประมวลผลข้อมูลส่วนบุคคลเพื่อการดำเนินกิจกรรมส่งเสริมการขายหรือการตลาดบางประเภทที่มีลักษณะเกินความคาดหมาย ที่อาจยังจะต้องอ้างอิงความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ ดังนั้น แนวปฏิบัติฉบับนี้จึงแนะนำให้บริษัทกำหนดและแยกส่วนที่เป็นการขอความยินยอมสำหรับวัตถุประสงค์เพื่อการดำเนินกิจกรรมส่งเสริมการขาย หรือการตลาดในลักษณะดังกล่าวออกจากส่วนอื่น เพื่อให้ลูกค้าได้รับแจ้งวัตถุประสงค์ดังกล่าวอย่างชัดเจน

5) การขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นได้อย่างชัดเจน

เงื่อนไขนี้มีจุดมุ่งหมายคือ การให้ความยินยอมนั้นเป็นไปได้อย่างชัดเจน และทำให้เจ้าของข้อมูลส่วนบุคคลไม่สับสน หรือเข้าใจผิดเกี่ยวกับการขอความยินยอมและขอบเขตของการขอ

⁴⁴ Recital 43 of the GDPR

ความยินยอมนั้น ซึ่งหากข้อความการขอความยินยอมนั้นขึ้นอยู่กับข้อสัญญา หรือเงื่อนไขในการให้บริการอื่น ๆ ก็อาจทำให้เจ้าของข้อมูลส่วนบุคคลสับสนระหว่างการตกลงให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเป็นส่วนหนึ่ง หรือเงื่อนไขของสัญญาหรือไม่ ดังนั้น การขอความยินยอมจะกระทำบนเอกสารเดียวกันกับหนังสือสัญญา หรือข้อตกลงการให้บริการใด ๆ ควรแยกส่วนการขอความยินยอมนั้นออกต่างหาก (อาจมีการทำกรอบหรือตัวอักษรที่มีลักษณะจำเพาะพิเศษ) ออกจากเนื้อหาส่วนอื่นของเอกสารทั้งหมด

6) ข้อความขอความยินยอมจะต้องใช้ภาษาที่อ่านง่าย เข้าใจได้ ไม่หลอกลวง และเข้าถึงได้ง่าย

เพื่อให้เป็นไปตามเงื่อนไขในการขอความยินยอมในข้อนี้ การขอความยินยอมควรมีลักษณะดังต่อไปนี้

- ใช้ภาษาที่อ่านเข้าใจง่าย และมีความหมายตรงไปตรงมา (Use Clear, Straightforward Language)
- ใช้ระดับ และรูปแบบของภาษาที่คงเส้นคงวา (Use Consistent Language)
- หลีกเลี่ยงการใช้คำศัพท์เฉพาะทางกฎหมาย หรือคำศัพท์ทางเทคนิคที่มีความหมายเฉพาะอื่น ตลอดจนวิธีการเขียนที่ทำให้สับสนในความหมาย เช่น ประโยคที่ประกอบด้วยการใช้ปฏิเสธซ้อนปฏิเสธ เป็นต้น
- พยายามให้คำขอความยินยอมมีขอบเขตชัดเจนและเฉพาะเจาะจงมากที่สุดเท่าที่จะทำได้ โดยควรพิจารณาได้ว่า เมื่อเจ้าของข้อมูลส่วนบุคคลอ่านแล้ว *สามารถ* คาดหมายได้ถึงกิจกรรมที่ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการ

ทั้งนี้ บริษัทยังจะต้องจัดให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงเนื้อหาข้อความการขอความยินยอมข้างต้นได้อย่างง่าย ซึ่งการเข้าถึงดังกล่าวอาจทำได้หลายรูปแบบ เช่น เอกสารอิเล็กทรอนิกส์ หรือเสียง เป็นต้น

ในส่วนของการเลือกใช้ภาษา แม้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ไม่ได้กำหนดว่าความยินยอมจะต้องเป็นภาษาไทยหรือภาษาอังกฤษ แต่บริษัทควรพิจารณาถึงกลุ่มเจ้าของข้อมูลส่วนบุคคลว่า บริษัทควรใช้ภาษาใดในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยให้เจ้าของข้อมูลส่วนบุคคลเข้าใจเนื้อหาของความยินยอมนั้น ๆ ได้ เช่น หากเจ้าของข้อมูลส่วนบุคคลเป็นคนไทย บริษัทควรขอความยินยอมเป็นภาษาไทย เป็นต้น

7) ในการขอความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงถึงความเป็นอิสระ ของเจ้าของข้อมูลส่วนบุคคล

ความยินยอมที่ให้โดยอิสระ (Freely Given) เป็นอีกหนึ่งเงื่อนไขของการขอความยินยอม กล่าวคือ ความยินยอมที่เจ้าของข้อมูลส่วนบุคคลให้นั้นต้องให้อย่างอิสระ เช่น ความยินยอมเพื่อการประมวลผลข้อมูลส่วนบุคคลที่ไม่มีความจำเป็น ในการเข้าทำสัญญาหรือให้บริการนั้นจะนำมากำหนดเป็นเงื่อนไขในการเข้าทำสัญญาหรือให้บริการไม่ได้

ทั้งนี้ หากข้อมูลส่วนบุคคลที่จะใช้ในการประมวลผลเป็นข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลดังกล่าวจำเป็นต้องประมวลผลเพื่อการเข้าทำสัญญาหรือเพื่อการปฏิบัติตามสัญญา (กรรมธรรม์ประกันภัย) บริษัทสามารถอ้างอิงฐานสัญญาได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอีก

5.1.1.2 การขอความยินยอม กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 20 กำหนดหลักเกณฑ์ในการขอความยินยอมของเจ้าของข้อมูลที่เป็นผู้เยาว์โดยใช้หลักการในการให้ความยินยอมของผู้เยาว์ที่สอดคล้องกับหลักเกณฑ์ที่กำหนดไว้ใน ป.พ.พ. ดังนี้

1) ความหมายผู้เยาว์

“บุคคลย่อมพ้นจากภาวะผู้เยาว์และบรรลุนิติภาวะเมื่ออายุยี่สิบปีบริบูรณ์”⁴⁵ โดยหากพิจารณา พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แล้วอาจแบ่งช่วงอายุของผู้เยาว์ได้ 2 ช่วง คือ อายุไม่เกิน 10 ปีและอายุตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์

2) หลักการทั่วไปเกี่ยวกับความสามารถในการกระทำที่มีผลทางกฎหมายของผู้เยาว์

“ผู้เยาว์จะทำนิติกรรมใด ๆ ต้องได้รับความยินยอมของผู้แทนโดยชอบธรรมก่อนการใด ๆ ที่ผู้เยาว์ได้ทำลงปราศจากความยินยอม เช่นว่านั้นเป็นโมฆียะเว้นแต่จะบัญญัติไว้เป็นอย่างอื่น”⁴⁶

⁴⁵ มาตรา 19 ป.พ.พ.

⁴⁶ มาตรา 21 ป.พ.พ.

หลัก ผู้เยาว์จะกระทำนิติกรรมใด ๆ ได้โดยได้รับความยินยอมโดยผู้แทนโดยชอบธรรมก่อน ซึ่งผู้แทนโดยชอบธรรมตามกฎหมายคือ บิดา มารดา ผู้ใช้อำนาจปกครอง หรือผู้มีอำนาจปกครองตามที่ศาลสั่ง

ข้อยกเว้น ผู้เยาว์อาจทำนิติกรรมเองได้โดยลำพัง ในกรณีดังต่อไปนี้ที่กฎหมายกำหนด

- ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อให้หลุดพ้นจากหน้าที่อันใดอันหนึ่ง
- เป็นการต้องทำเองเฉพาะตัว
- เป็นการสมแก่ฐานะานุรูปแห่งตนและเป็นการอันจำเป็นในการดำรงชีพตามสมควร

ผลของการฝ่าฝืน นิติกรรมที่กระทำให้โดยฝ่าฝืนนั้นตกเป็นโมฆียะ สามารถถูกบอกล้างได้

3) หลักการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 20 ได้กำหนดช่วงอายุที่ต้องพิจารณาในการขอความยินยอมของผู้เยาว์ ในกรณีดังต่อไปนี้

กรณีผู้เยาว์มีอายุตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์

หลัก ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ที่ไม่เกี่ยวข้องกับนิติกรรมที่ได้รับการยกเว้นตาม ป.พ.พ. ดังกล่าวข้างต้นแล้ว เจื่อนใจในการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ มีดังต่อไปนี้

- ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ และ
- ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองของเจ้าของข้อมูลส่วนบุคคล (ผู้เยาว์) และ

- การขอความยินยอมนี้ต้องเป็นไปตามเงื่อนไขการขอความยินยอมทั่วไปที่ได้อธิบายไว้แล้วข้างต้นด้วย

ข้อยกเว้น บริษัทสามารถขอความยินยอมจากผู้เยาว์แต่เพียงผู้เดียวได้ หากเป็นนิติกรรมที่ผู้เยาว์สามารถเข้าทำเองได้ตามที่กำหนดใน ป.พ.พ. ข้างต้น

กรณีผู้เยาว์มีอายุไม่เกิน 10 ปี

ในกรณีเจ้าของข้อมูลส่วนบุคคลที่ผู้เยาว์อายุไม่เกิน 10 ปี ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองของเจ้าของข้อมูลส่วนบุคคลคนนั้นเสมอ โดยไม่มีข้อยกเว้น โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการขอความยินยอมตามเงื่อนไขการขอความยินยอมทั่วไปใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 19 ที่ได้อธิบายมาข้างต้นแล้วด้วย

ข้อสังเกต

- ในการขอความยินยอมเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์นั้น บริษัทจะต้องจัดให้การขอความยินยอมเป็นไปตามเงื่อนไขทั่วไปใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 19 ด้วย
- หากสามารถอ้างอิงฐานโดยชอบด้วยกฎหมายอื่น ในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ได้ บริษัทไม่จำเป็นต้องขอความยินยอมจากผู้เยาว์และผู้ใช้อำนาจปกครองของผู้เยาว์ เช่น บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เยาว์เนื่องจากผู้เยาว์ถูกระบุเป็นผู้รับประโยชน์ในกรรมธรรม์ประกันภัย เช่นนี้การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์สามารถอ้างอิงฐานประโยชน์อันชอบธรรมได้ บริษัทไม่จำเป็นต้องขอความยินยอมจากผู้เยาว์ และ/หรือ ผู้ใช้อำนาจปกครอง

4) สรุปแนวทางการพิจารณาในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้เยาว์

หากผู้ประมวลผลข้อมูลส่วนบุคคลเห็นว่า จะต้องประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ สิ่ง que บริษัทต้องคำนึงถึงมีดังต่อไปนี้

วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์

บริษัทต้องพิจารณาวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเพื่อกำหนดฐานในการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลก่อน

หากการประมวลผลข้อมูลส่วนบุคคลไม่จำเป็นต้องอ้างอิงฐานความยินยอม บริษัทก็ไม่ต้องขอความยินยอมจากผู้เยาว์ เช่น บริษัทประมวลผลข้อมูลส่วนบุคคล (ไม่รวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว) ของผู้เยาว์เพื่อการรับประกันภัย ซึ่งการประมวลผลข้อมูลส่วนบุคคลเพื่อการรับประกันภัยสามารถอ้างอิงฐานสัญญาได้ ไม่จำเป็นต้องขอความยินยอมจากผู้เยาว์ (เจ้าของข้อมูลส่วนบุคคล)

ข้อสังเกต

แม้บริษัทไม่ต้องขอความยินยอมจากผู้เยาว์ เจ้าของข้อมูลส่วนบุคคล บริษัทยังมีหน้าที่อื่นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เช่น หน้าที่ในการแจ้งรายละเอียดตามมาตรา 23 หน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น

ตัวอย่างที่ 1 นางสาว ก. อายุ 18 สมักรซื้อประกันภัยอุบัติเหตุส่วนบุคคลบนเว็บไซต์ของบริษัท ค. การที่นางสาว ก. สมักรซื้อประกันภัยด้วยตนเอง และเมื่อบริษัท ค. ทำการประมวลผลข้อมูลส่วนบุคคลของนางสาว ก. เพื่อพิจารณาคำนวณเบี้ยประกันภัย เช่นนี้ เป็นกรณีที่บริษัท ค. จำเป็นต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของนางสาว ก. ก่อนเข้าทำสัญญาประกันภัย ซึ่งบริษัท ค. สามารถอ้างอิงฐานสัญญาเพื่อประมวลผลข้อมูลส่วนบุคคลของนางสาว ก. ได้

ตัวอย่างที่ 2 นาง ก. มารดาของเด็กหญิง ข. ซื้อประกันภัยอุบัติเหตุการเดินทางของบริษัท ค. ให้แก่เด็กหญิง ข. อายุ 5 ปี (ผู้เยาว์) โดยนาง ก. มารดาเป็นผู้ระบุรายละเอียดเกี่ยวกับเด็กหญิง ข. ทั้งหมด ให้บริษัท ค. เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของเด็กหญิง ข. เพื่อพิจารณาคำนวณเบี้ยประกันภัยของเด็กหญิง ข. เช่นนี้เป็นกรณีที่บริษัท ค. ประมวลผลข้อมูลส่วนบุคคลของเด็กหญิง ข. ซึ่งเป็นข้อมูลที่ได้มาจากจากนาง ก. ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล

ในกรณีข้อเท็จจริงสมมุตินี้ต้องพิจารณาการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคล

กรณีนี้บริษัท ค. เก็บรวบรวมข้อมูลส่วนบุคคลของเด็กหญิง ข. มาจากนาง ก. มารดา ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล ดังนั้น ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 25 ห้ามไม่ให้เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล เว้นแต่การประมวลผลข้อมูลส่วนบุคคลนั้นได้รับข้อยกเว้นไม่ต้องขอความยินยอม กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลอยู่บนฐานโดยชอบด้วยกฎหมายอื่นนอกจากฐานความยินยอม ดังนั้น ในกรณีนี้ การประมวลผลข้อมูลส่วนบุคคลของเด็กหญิง ข. นั้นเป็นไปเพื่อประกอบการทำกรรมธรรม์ประกันภัย และการจ่ายค่าสินไหมทดแทนในอนาคต ซึ่งอาจอ้างอิงฐานประโยชน์อันชอบธรรมได้ ดังนั้น บริษัท ค. สามารถเก็บรวบรวมข้อมูลส่วนบุคคลของเด็กหญิง ข. จากนาง ก. มารดาได้

ข้อสังเกต

กรณีนี้ บริษัท ค. ไม่สามารถอ้างอิงฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลของเด็กหญิง ข. ได้ เนื่องจากการประมวลผลที่สามารถอ้างอิงฐานสัญญาได้ จะต้องเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามคำขอในก่อนเข้าทำสัญญา ของเจ้าของข้อมูลส่วนบุคคล (เด็กหญิง ข.) เท่านั้น

การประมวลผลข้อมูลส่วนบุคคลของนาง ก.

ด้วยเหตุที่นาง ก. เป็นผู้สมัครขอเอาประกันภัยให้เด็กหญิง ข. นาง ก. จึงอาจจะต้องให้ข้อมูลส่วนบุคคลของตนกับบริษัท ค. และเมื่อบริษัท ค. ทำการประมวลผลข้อมูลส่วนบุคคลของนาง ก. เพื่อใช้ในการติดต่อทำสัญญาประกันภัยกับเด็กหญิง ข. เช่นนี้ บริษัท ค. สามารถอ้างอิงฐานประโยชน์อันชอบธรรม (Legitimate Interest) ในการประมวลผลข้อมูลส่วนบุคคลของนาง ก. ได้ โดยไม่ต้องขอความยินยอมจากนาง ก. อีก

อายุของผู้เยาว์

หากการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ไม่อาจอ้างอิงฐานอื่นนอกจากฐานความยินยอมได้ สิ่ง que บริษัทต้องพิจารณาต่อไปคืออายุของเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดวิธีการขอความยินยอมของผู้เยาว์ที่แตกต่างกันไปตามช่วงอายุ ดังรายละเอียดข้างต้น

5.1.1.3 ข้อสังเกตและข้อควรระวังเกี่ยวกับการขอความยินยอม

ความยินยอมมีระยะเวลาอยู่ได้นานเท่าใด

แม้ว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจะไม่ได้กล่าวถึงระยะเวลาของความสมบูรณ์ของความยินยอมไว้ แต่ในทางปฏิบัติแล้ว บริษัทจะต้องพิจารณาจากข้อเท็จจริงเกี่ยวกับการให้ความยินยอม และวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่ได้รับความยินยอม (พิจารณาว่าความยินยอมที่ได้มีขอบเขตให้ดำเนินการได้เท่าใด) กล่าวคือ หากบริษัทมีการเปลี่ยนแปลงวิธีการดำเนินธุรกิจที่ส่งผลให้วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลเปลี่ยนไป จนทำให้ความยินยอมที่ให้ไว้เดิมไม่เพียงพอให้ใช้ได้กับวัตถุประสงค์ใหม่ที่เปลี่ยนไป เพราะถือว่าเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้แก่วัตถุประสงค์ในการประมวลผลข้อมูลเดิมเท่านั้นไม่ใช่วัตถุประสงค์ใหม่ ดังนั้น เมื่อมีการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ใหม่ที่ต้องใช้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล บริษัทก็ต้องขอความยินยอมใหม่สำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมใหม่

นอกจากนี้ความยินยอมอาจหมดไปตามสภาพได้อีกด้วย เช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมไว้สำหรับการประมวลผลเพื่อวัตถุประสงค์การวิเคราะห์สำรวจทางการตลาดในปี 2563 เมื่อการทำการดำเนินการดังกล่าวสิ้นสุดลง โดยสภาพแล้วความยินยอมนั้นย่อมหมดไป

5.1.2 ฐานสัญญา (Contractual Necessity)

ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล⁴⁷ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงฐานสัญญาเป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ เมื่อการประมวลผลข้อมูลส่วนบุคคลมีลักษณะดังต่อไปนี้

5.1.2.1 ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ตามแนวทางการพิจารณาของ ICO ซึ่งเป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยตีความคำว่า “จำเป็น” ในกรณีนี้ ตามหลักของ GDPR ว่า ความจำเป็นนั้นไม่จำกัดแต่เพียงว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นมีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลโดยไม่มีทางอื่นที่จะปฏิบัติตามสัญญาได้เท่านั้น แต่ขยายความรวมถึงเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเห็นสมควรว่า การประมวลผล

⁴⁷ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมาตรา 24(3)

ข้อมูลส่วนบุคคลนั้นเป็นส่วนสำคัญเพื่อให้สามารถดำเนินการตามคำขอก่อนเข้าทำสัญญาหรือเพื่อให้สามารถปฏิบัติตามสัญญาได้ ทั้งนี้ การประมวลผลข้อมูลโดยใช้ความเห็นของผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะต้องเฉพาะเจาะจงและได้สัดส่วนด้วย⁴⁸

ตัวอย่าง

บริษัท ค. เสนอขายประกันภัยอุบัติเหตุผ่านทางช่องทางออนไลน์ โดยมีการระบุให้ผู้มุ่งหวังเอาประกันภัยหรือลูกค้า ต้องให้รายละเอียดเกี่ยวกับอีเมล เพื่อที่บริษัทจะสามารถติดต่อสอบถามข้อมูลเพิ่มเติม หรือขอเอกสารอื่น ๆ ที่เกี่ยวข้องเพิ่มเติม พร้อมทั้งออกใบเสนอราคาประกันภัยสุขภาพให้ลูกค้าทางอีเมลต่อไป เช่นนี้ เป็นกรณีที่บริษัทมีความจำเป็นที่จะต้องประมวลผลข้อมูลส่วนบุคคลเพื่อที่จะได้สามารถดำเนินการตามคำขอก่อนเข้าทำสัญญาของผู้มุ่งหวังหรือลูกค้า โดยใช้ข้อมูลส่วนบุคคลดังกล่าวในการติดต่อสอบถามและส่งใบเสนอราคาเบี้ยประกันภัยได้

5.1.2.2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปเพื่อวัตถุประสงค์ดังต่อไปนี้

1) เพื่อดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา

เมื่อพิจารณาถ้อยคำในกฎหมายแล้ว จะสังเกตได้ว่า กฎหมายมุ่งเน้นให้วัตถุประสงค์ในกรณีนี้จำกัดอยู่เพียงกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้ร้องขอหรือมีคำขอมายังผู้ควบคุมข้อมูลส่วนบุคคล (บริษัท) เพื่อให้ดำเนินการบางอย่างก่อนที่จะเข้าทำสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยไม่รวมถึงกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้เสนอหรือร้องขอ⁴⁹

ตัวอย่าง นาย ก. ติดต่อบริษัท ค. เพื่อสอบถามรายละเอียดเกี่ยวกับกรมธรรม์ประกันภัยที่อยู่อาศัยของนาย ก. พร้อมทั้งร้องขอให้บริษัท ค. ประเมินราคาเบี้ยประกันภัยให้กับตน กรณีนี้ บริษัท ค. มีความจำเป็นที่จะต้องประมวลผลข้อมูลส่วนบุคคลของนาย ก. เช่น ชื่อ-นามสกุล ที่อยู่ เพศ อายุ เพื่อคำนวณเบี้ยประกันภัยและเสนอราคาให้กับนาย ก. ตามคำขอเอาประกันภัยที่อยู่อาศัยข้างต้นของนาย ก. ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล ก่อน

⁴⁸ Information Commissioner's Office, UK (ICO), 'When is processing 'necessary' for a contract?', ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract> > accessed 12 April 2020

⁴⁹ Information Commissioner's Office, UK (ICO), 'Contract', ICO <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/>> accessed 12 April 2020

จะทำสัญญาประกันภัย ดังนั้น การประมวลผลข้อมูลส่วนบุคคลของนาย ก. จึงอ้างอิงฐานสัญญาได้

2) เพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา

การประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อการปฏิบัติตามสัญญานั้น ต้องเป็นกรณีที่มีสัญญาอยู่แล้วระหว่างผู้ควบคุมข้อมูลส่วนบุคคล (บริษัท) กับเจ้าของข้อมูลส่วนบุคคล และการประมวลผลข้อมูลส่วนบุคคลดังกล่าวเป็นไปเพื่อการดำเนินงานให้เป็นไปตามสัญญาที่มีอยู่ หรือเพื่อปฏิบัติตามสิทธิหน้าที่ตามสัญญาเท่านั้น

ตัวอย่าง ภายหลังนาย ก. ซื้อประกันภัยอุบัติเหตุกับบริษัท ข. แล้ว นาย ก. ประสบอุบัติเหตุต้องเข้าโรงพยาบาล บริษัท ข. มีหน้าที่ที่จะต้องจ่ายค่าสินไหมทดแทนให้แก่ นาย ก. ตามกรมธรรม์ประกันอุบัติเหตุ ดังนี้ บริษัท ข. จึงมีความจำเป็นที่จะต้องประมวลผลข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ เลขบัญชีธนาคารของนาย ก. ซึ่งเป็นผู้เอาประกันภัยเพื่อดำเนินการจ่ายค่าสินไหมทดแทนตามกรมธรรม์ประกันภัย ซึ่งเป็นการประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อปฏิบัติตามสัญญาที่มีอยู่ระหว่างผู้ควบคุมข้อมูล (บริษัท ข.) กับเจ้าของข้อมูลส่วนบุคคล (นาย ก)

ข้อควรพิจารณา ในกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยอ้างอิงฐานสัญญา บริษัทผู้ควบคุมข้อมูลส่วนบุคคลควรจะต้องประเมินขอบเขตสิทธิและหน้าที่ตามสัญญาประกันภัยระหว่างบริษัทกับเจ้าของข้อมูลส่วนบุคคลให้ชัดเจน เมื่อบริษัททราบแล้วว่าขอบเขตของการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานสัญญานั้นมีขอบเขตเท่าใด บริษัท ก็สามารถป้องกันไม่ให้มีการอ้างอิงฐานสัญญาเพื่อประมวลผลข้อมูลส่วนบุคคลนอกขอบเขตของสิทธิหน้าที่ตามสัญญาที่มีอยู่ และเลือกใช้ฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่นได้อย่างถูกต้องตามกฎหมาย

ข้อสังเกต

- เมื่อการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามฐานสัญญา บริษัทไม่จำเป็นต้องมีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อการดำเนินการตามวัตถุประสงค์เดียวกันนี้อีก
- การประมวลผลข้อมูลบนฐานสัญญานี้จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สาม เช่น การประมวลผลข้อมูลของผู้รับประโยชน์ในสัญญาประกันภัย จะกระทำโดยอ้างอิงฐานสัญญาไม่ได้ เพราะผู้รับประโยชน์ไม่ใช่คู่สัญญากับบริษัท ทั้งนี้ หาก

เป็นการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่สาม บริษัทต้องอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่นนอกจากฐานสัญญา เช่น ฐานความยินยอม หรือฐานประโยชน์อันชอบธรรม แล้วแต่กรณี

- ฐานสัญญานี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น แต่ไม่สามารถใช้อ้างอิงในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ได้ เนื่องจากฐานโดยชอบด้วยกฎหมายในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น แตกต่างไปจากฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป

ข้อควรระวังเกี่ยวกับการวิเคราะห์ข้อมูล (Data Analysis) เพื่อดำเนินธุรกิจของบริษัท หรือเพื่อการกระทำที่เป็นการส่งเสริมการขาย

ตามที่ได้อธิบายไว้แล้วเบื้องต้นเกี่ยวกับการอ้างอิงฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลว่า บริษัทสามารถอ้างอิงฐานสัญญาในการประมวลผลข้อมูลได้ หากบริษัทจะต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญาหรือคำขอของผู้มุ่งหวังเอาประกันภัยก่อนสัญญา เช่น การประมวลผลข้อมูลอายุของผู้ขอเอาประกันภัยเพื่อกำหนดเบี้ยประกันภัย หรือการประมวลผลข้อมูลที่อยู่เพื่อจัดส่งกรมธรรม์ประกันภัย เป็นต้น

อย่างไรก็ดี หากเป็นการประมวลผลข้อมูลส่วนบุคคลที่ทำเพื่อประโยชน์ในการดำเนินธุรกิจของบริษัทตามวัตถุประสงค์อื่น บริษัทจะไม่สามารถอ้างอิงฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลเพื่อการนั้นได้ แม้จะมีการกำหนดไว้ในข้อสัญญาก็ตาม เช่น กรณีบริษัทนำรายละเอียดข้อมูลส่วนบุคคลของผู้มุ่งหวังเอาประกันภัยไปเปิดเผยกับคู่ค้าเพื่อให้คู่ค้าทำกิจกรรมที่เป็นการส่งเสริมการขาย เช่น การทำการตลาดทางตรง (Direct Marketing) การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุ้นยอดขาย (Social Network) การโฆษณาออนไลน์แบบเฉพาะเจาะจง (Online Targeting Advertisement) เป็นต้น

ดังนั้น หากบริษัทต้องการจะประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ในการดำเนินธุรกิจของบริษัท หรือเพื่อประกอบกิจกรรมการส่งเสริมการขายดังกล่าว บริษัทต้องอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลอื่นนอกจากฐานสัญญา เช่น ฐานความยินยอม ฐานประโยชน์อันชอบธรรม เป็นต้น และหากบริษัทอ้างอิงฐานความยินยอม ในการขอความยินยอมนั้น บริษัทต้องระบุวัตถุประสงค์อย่างชัดเจน และทำการขอความยินยอมตามหลักเกณฑ์การขอความยินยอมที่ได้อธิบายไว้แล้วข้างต้นตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 19 โดยบริษัทจะต้องระมัดระวังการตั้งค่าเริ่มต้น (Default) ไม่ให้ “เลือก” ให้ความยินยอมในวัตถุประสงค์ดังกล่าวไว้ก่อน แต่บริษัทต้องให้เจ้าของข้อมูลส่วนบุคคลเป็นผู้ “เลือก” ให้ความยินยอมแก่วัตถุประสงค์นั้นเอง โดยเฉพาะอย่างยิ่งการให้ความยินยอมต่อ

การประมวลผลข้อมูลส่วนบุคคลเพื่อประกอบกิจกรรมส่งเสริมการขายผ่านทางช่องทางอิเล็กทรอนิกส์

5.1.2.3 แนวทางในการพิจารณาการประมวลผลข้อมูลส่วนบุคคลตามฐานสัญญา

ในการพิจารณาการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานสัญญา สิ่งที่บริษัทหรือผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณาเป็นอย่างแรกคือ การประเมินขอบเขตสิทธิและหน้าที่ตามกรรมธรรม์ประกันภัยของบริษัทที่มีกับลูกค้า คู่สัญญา หรือบุคคลอื่น ๆ ให้ชัดเจน เพื่อให้ทราบว่าขอบเขตของการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานสัญญานั้นมีขอบเขตเท่าใดเพื่อหากมีการประมวลผลข้อมูลส่วนบุคคลนอกขอบเขตของสิทธิหน้าที่ตามสัญญา บริษัทจะได้ดำเนินการตามกฎหมายอย่างถูกต้อง

(1) ข้อมูลที่จำเป็นต้องมีในการเข้าทำสัญญาหมายถึงข้อมูลส่วนบุคคลประเภทใดบ้าง บริษัทต้องพิจารณาอย่างไร

ขอบเขตของฐานสัญญาคือ ข้อมูลส่วนบุคคลที่จำเป็นต้องใช้เพื่อ (1) เข้าทำสัญญา เช่นข้อมูลที่ต้องใช้เพื่อประกอบการพิจารณารับประกันภัย ทั้งนี้ ขึ้นอยู่กับประเภทของผลิตภัณฑ์ของบริษัท ว่าในแต่ละผลิตภัณฑ์ หรือแต่ละกรณี บริษัทจำเป็นต้องใช้ข้อมูลส่วนบุคคลใดบ้าง หรือ (2) ข้อมูลที่จำเป็นเพื่อการปฏิบัติหน้าที่ตามสัญญา

ทั้งนี้ เนื่องจากฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวกับฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไปต่างกัน แม้บริษัทจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อใช้ในการเข้าทำสัญญา บริษัทก็ยังคงต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่สามารถอ้างอิงข้อยกเว้นอื่นตามกฎหมาย

(2) บริษัทสามารถส่งข้อมูลลูกค้าไปให้บริษัทประกันต่อ โดยใช้อ้างอิงตามฐานสัญญาได้หรือไม่ กล่าวคือ กรณีประกันภัยต่อ เป็นกระบวนการส่วนหนึ่งในธุรกิจประกันภัย ควรอ้างอิงฐานสัญญาได้หรือไม่

การส่งข้อมูลส่วนบุคคลไปให้บริษัทประกันภัยต่อ เป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานประโยชน์อันชอบธรรม เนื่องจากการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานสัญญา ต้องเป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาเท่านั้น ซึ่งสัญญาประกันภัยต่อลูกค้ามิได้เป็นคู่สัญญา บริษัทจึงอ้างอิงฐานสัญญาสำหรับการดำเนินการประกันภัยต่อไม่ได้

ในกรณีของข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ประวัติสุขภาพ การประมวลผลรวมถึงการส่งข้อมูลดังกล่าวให้บริษัทประกันภัยต่อ จะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่สามารถอ้างอิงข้อยกเว้นอื่นตามกฎหมาย

5.1.3 ฐานประโยชน์ที่สำคัญต่อชีวิต (Vital Interest)

ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงฐานประโยชน์ที่สำคัญต่อชีวิต ในการประมวลผลข้อมูลส่วนบุคคลได้ เมื่อมีความจำเป็นที่จะต้องประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ดังต่อไปนี้เท่านั้น⁵⁰

- ระวังอันตรายต่อชีวิต
- ระวังอันตรายต่อร่างกาย
- ระวังอันตรายต่อสุขภาพของบุคคล

ตัวอย่าง

- บริษัทอาจเปิดเผยข้อมูลโรคประจำตัวของผู้อุปถัมภ์ภัยอุบัติเหตุต่อโรงพยาบาลได้เพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการรักษาอย่างเร่งด่วนและหมดสติ
- โรงพยาบาลอาจประมวลผลข้อมูลของบิดามารดาเพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของบุตร เช่น ต้องมีการพิจารณาถึงโรคทางพันธุกรรมของบุตรที่เป็นทารก เป็นต้น

ข้อสังเกต

การประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานเพื่อประโยชน์ที่สำคัญต่อชีวิตนั้นมีขอบเขตที่จำกัดมาก หากพิจารณาเจตนารมณ์ของกฎหมายแล้ว ฐานในการประมวลผลข้อมูลส่วนบุคคลนี้มุ่งใช้กับกรณีที่เป็นกรณีฉุกเฉิน หรือเป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนได้

ทั้งนี้ บริษัทไม่สามารถอ้างอิงฐานประโยชน์ที่สำคัญต่อชีวิต เพื่อทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์สำหรับการพิจารณาจ่ายสินไหมทดแทน เพราะการพิจารณาจ่ายสินไหมทดแทน ไม่ใช่การระวังอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล แต่อาจ

⁵⁰ มาตรา 24(2) พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

อ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคล ฐานอื่นได้ เช่น ฐานสัญญา หรือฐานประโยชน์อันชอบธรรม เป็นต้น

5.1.4 ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

การประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานหน้าที่ตามกฎหมายนั้น รองรับการนี้ที่ผู้ควบคุมข้อมูลส่วนบุคคล (บริษัท) มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อการดำเนินการให้เป็นไปตามบทบัญญัติตามกฎหมายหรือตามคำสั่งโดยชอบด้วยกฎหมายของหน่วยงานของรัฐ เช่น สำนักงาน คปภ. สำนักงาน ปปง. คำสั่งศาล หรือเจ้าหน้าที่รัฐที่ได้รับมอบหมายให้ดำเนินการตามที่กฎหมายกำหนด ดังนั้น ในกรณีที่ บริษัทอ้างอิงฐานหน้าที่ตามกฎหมายนี้ บริษัทผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุได้ว่า บริษัทมีความจำเป็นต้องปฏิบัติหน้าที่ตามกฎหมายข้อใด ฉบับใด หรือตามคำสั่งโดยชอบด้วยกฎหมายของหน่วยงานรัฐหน่วยงานใด⁵¹

อย่างไรก็ตาม หากเป็นกรณีที่บริษัท ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเลือกกระหว่างการประมวลผลข้อมูลส่วนบุคคล กับใช้วิธีอื่นที่เหมาะสม เพื่อให้บริษัทสามารถปฏิบัติหน้าที่ตามกฎหมายได้ ดังนี้ ถือว่าบริษัทไม่มีความจำเป็นและไม่สามารถอ้างอิงฐานหน้าที่ตามกฎหมายในการประมวลผลข้อมูลส่วนบุคคลได้ ดังนั้น บริษัทจะต้องพิจารณาความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติหน้าที่ตามกฎหมาย ก่อนจึงจะระบุว่าการประมวลผลข้อมูลส่วนบุคคลดังกล่าวเป็นไปเพราะความจำเป็นในการปฏิบัติตามกฎหมายหรือไม่

ตัวอย่าง

- สำนักงาน คปภ. กำหนดให้บริษัทต้องส่งข้อมูลส่วนบุคคลของลูกค้าเกี่ยวกับการรับประกันภัยและการจ่ายค่าสินไหมทดแทนผ่านระบบ IBS ตามแบบที่สำนักงาน คปภ. กำหนด
- บริษัทมีหน้าที่รายงานธุรกรรมตามที่กฎหมายกำหนด หรือรายงานธุรกรรมที่ต้องสงสัย ซึ่งประกอบไปด้วยข้อมูลส่วนบุคคลของลูกค้าต่อ สำนักงาน ปปง. ภายใต้ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน

⁵¹ มาตรา 24(6) พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และRecital 41 of the GDPR

แนวทางในการดำเนินการเมื่อมีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานหน้าที่ตามกฎหมาย

ในกรณีที่บริษัทจะต้องประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อดำเนินการให้เป็นไปตามหน้าที่ตามกฎหมาย บริษัทอาจจัดให้มีแนวทางปฏิบัติ ดังต่อไปนี้

- ระบรวมวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล และฐานในการประมวลผลข้อมูลนี้ลงในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
- ระบุงบข้อกฎหมายหรือคำสั่งของหน่วยงานที่เป็นเหตุทำให้มีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล โดยอ้างอิงฐานหน้าที่ตามกฎหมาย
- จัดให้มีการบันทึกเกี่ยวกับเหตุผลความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล โดยอ้างอิงฐานหน้าที่ตามกฎหมาย

5.1.5 ฐานภารกิจของรัฐ (Public Task)

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อปฏิบัติหน้าที่ในการดำเนินการกิจประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจที่ได้รับมอบหมายจากรัฐ⁵² ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงฐานภารกิจของรัฐ เพื่อใช้เป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ ทั้งนี้ โดยส่วนมาก ฐานภารกิจของรัฐนี้มักจะถูกอ้างอิงโดยผู้ควบคุมข้อมูลส่วนบุคคลที่มีสถานะเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงาน คปภ. สำนักงานศาลปกครอง สำนักงานปปง. เจ้าหน้าที่ของกระทรวงต่าง ๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ดำเนินการโดยใช้อำนาจตามที่รัฐได้มอบหมาย เช่น การให้บริการสอบใบขับขี่ ให้บริการสอบใบอนุญาตตัวแทนหรือนายหน้าประกันวินาศภัย อนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องสามารถอ้างอิงกฎหมายอันเป็นที่มาของอำนาจหน้าที่ที่เป็นภารกิจของรัฐได้อย่างชัดเจน ดังนั้น กรณีที่บริษัทจะมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล โดยอ้างอิงภารกิจของรัฐนี้จึงอาจเกิดขึ้นได้น้อยมาก

การประมวลผลข้อมูลส่วนบุคคลโดยใช้ฐานภารกิจของรัฐนี้ไม่สามารถใช้อ้างอิงได้ หากปรากฏข้อเท็จจริงว่า การปฏิบัติภารกิจของรัฐนั้นสามารถดำเนินการได้โดยไม่จำเป็นต้องมีการประมวลผลข้อมูลส่วนบุคคล เช่น สำนักงาน คปภ. สามารถตรวจสอบข้อมูลทางตลาดประกันวินาศภัยในภาพรวม ได้โดย

⁵² มาตรา 24(4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ไม่ต้องประมวลผลข้อมูลส่วนบุคคลที่เชื่อมโยงไปถึงตัวตนของเจ้าของข้อมูลส่วนบุคคลแต่ละคน เพียงแต่วิเคราะห์ข้อมูลสถิติที่ไม่มีข้อมูลส่วนบุคคลของผู้เอาประกันภัยที่บริษัทส่งให้ สำนักงาน คปภ. ก็เพียงพอ⁵³

อนึ่ง เจ้าของข้อมูลจะไม่มีสิทธิในการขอให้ลบ หรือคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่มีการอ้างอิงฐานภารกิจของรัฐนี้ เพื่อประมวลผลข้อมูลส่วนบุคคล

แนวทางในการดำเนินการเมื่อมีการประมวลผลข้อมูลส่วนบุคคลตามฐานภารกิจของรัฐ

ในกรณีที่บริษัทจะทำการประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อดำเนินการตามภารกิจของรัฐ บริษัทควรจัดให้มีแนวปฏิบัติ ดังต่อไปนี้

- ระบุมววัตถุประสงค์ในการประมวลผลข้อมูล และฐานในการประมวลผลข้อมูลนี้ลงในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Protection Policy) ของบริษัท
- ระบุภารกิจ หน่วยงาน และข้อกำหนดที่ให้อำนาจให้มีการดำเนินการของรัฐ หรือกฎหมายที่เกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคลเพื่อการดำเนินการตามภารกิจของรัฐในแต่ละกรณี
- จัดให้มีการบันทึกเกี่ยวกับเหตุผลความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลที่อ้างอิงฐานภารกิจของรัฐ

ข้อสังเกต ในกรณีที่หน่วยงานของรัฐร้องขอให้บริษัทส่งข้อมูลส่วนบุคคลเพื่อดำเนินการอย่างใดอย่างหนึ่ง บริษัทอาจไม่สามารถอ้างอิงฐานภารกิจของรัฐได้ทุกกรณี และบริษัทอาจจะต้องอ้างอิงฐานอื่น เช่น หน้าที่ตามกฎหมาย หรือประโยชน์โดยชอบด้วยกฎหมาย แล้วแต่กรณี เพราะในบางกรณีอาจเป็นการร้องขอความร่วมมือมากกว่ากรณีร้องขอโดยอาศัยอำนาจตามกฎหมาย ดังนั้น ก่อนที่บริษัทจะดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำร้องขอ บริษัทควรสอบถามหรือตรวจสอบอำนาจหน้าที่ของหน่วยงานของรัฐ หรือเจ้าหน้าที่รัฐนั้น ๆ ทุกครั้ง

5.1.6 ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นที่จะต้องทำการประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงฐานประโยชน์อันชอบธรรม เป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (5)

⁵³ ปิยะบุตร บุญอร่ามเรือง พิรพัฒน์ โชคสุวัฒนสกุล ปิติ เอี่ยมจารุญลาภ ชวิน อุณหัทร และฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, Thailand Data Protection Guidelines 2.0 : แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, หน้า 77, โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, ตุลาคม 2562

อย่างไรก็ตาม หากประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล จะอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลนี้ไม่ได้

การอ้างอิงฐานประโยชน์อันชอบธรรม มีเงื่อนไขดังต่อไปนี้

- 1) การประมวลผลข้อมูลส่วนบุคคลเป็นไปเพราะความจำเป็นเพื่อประโยชน์ของบุคคลดังต่อไปนี้
 - ผู้ควบคุมข้อมูลส่วนบุคคล
 - บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล
- 2) ประโยชน์ของบุคคลดังกล่าว ต้องเป็นประโยชน์โดยชอบด้วยกฎหมายเท่านั้น กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลนั้น ๆ จะต้องไม่เป็นการฝ่าฝืนกฎหมายใด ๆ หรืออาจเป็นกรณีที่อยู่ในขอบเขตที่กฎหมายอนุญาตให้ทำได้
- 3) ประโยชน์โดยชอบด้วยกฎหมายของบุคคลดังกล่าวต้องไม่มีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานที่เกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิในความเป็นส่วนตัว สิทธิในชื่อเสียง เป็นต้น

จากเงื่อนไขข้างต้นจะสังเกตได้ว่า ฐานประโยชน์อันชอบธรรม มีขอบเขตในการปรับใช้ที่ค่อนข้างกว้างและยืดหยุ่น ไม่มีวัตถุประสงค์หรือขอบเขตกำหนดไว้โดยเฉพาะเจาะจงและชัดเจนเหมือนฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่น ดังเช่นฐานหน้าที่ตามกฎหมายที่มีการกำหนดขอบเขตของฐานในการประมวลผลอย่างชัดเจนว่าใช้เพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ตามกฎหมายเท่านั้น

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ดุลยพินิจซึ่งน้ำหนักความสำคัญระหว่างประโยชน์โดยชอบด้วยกฎหมายและสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อเป็นเช่นนั้นแล้ว บริษัทจะต้องระมัดระวังในการใช้ดุลยพินิจซึ่งน้ำหนักความสำคัญระหว่างประโยชน์และสิทธิดังกล่าวเป็นอย่างมาก เพราะมีความเสี่ยงสูงที่จะเกิดข้อโต้แย้งจากเจ้าของข้อมูลส่วนบุคคล

ในส่วนของสิทธิขั้นพื้นฐานนั้น ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 กำหนดสิทธิขั้นพื้นฐานของประชาชนชาวไทยไว้ดังนี้⁵⁴

⁵⁴ สำนักวิชาการ สำนักเลขาธิการสภาผู้แทนราษฎร, สรุปสาระสำคัญรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560, <<https://library2.parliament.go.th/ebook/content-ebbas/2560-bas.pdf>> เข้าถึงเมื่อวันที่ 13 เมษายน 2563

1. สิทธิและเสรีภาพในชีวิตและร่างกาย
2. สิทธิในกระบวนการยุติธรรมทางอาญา
3. สิทธิในการไม่ถูกเกณฑ์แรงงาน
4. สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว
5. สิทธิในทรัพย์สินและการสืบมรดก
6. สิทธิของผู้บริโภคในการรวมกันจัดตั้งองค์กรของผู้บริโภคเพื่อคุ้มครองและพิทักษ์สิทธิของผู้บริโภค
7. สิทธิในการได้รับการบริการสาธารณสุข
8. สิทธิในการได้รับความช่วยเหลือจากรัฐของผู้เป็นมารดา บุคคลซึ่งมีอายุเกิน 60 ปี และไม่มีรายได้เพียงพอแก่การยังชีพ และบุคคลผู้ยากไร้

ทั้งนี้ ในกรณีที่มีการอ้างอิงฐานประโยชน์อันชอบธรรมนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้พิจารณาเพียง **สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคล** ของเจ้าของข้อมูลส่วนบุคคลเท่านั้น ดังนั้น การพิจารณาสิทธิขั้นพื้นฐานในกรณีนี้ จึงจำกัดอยู่เพียงแค่สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลเท่านั้น เช่น สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง เป็นต้น ไม่รวมสิทธิขั้นพื้นฐานอื่น ๆ

แนวทางการพิจารณาการใช้ฐานประโยชน์อันชอบธรรม

ก่อนที่บริษัทจะกำหนดว่ากิจกรรมการประมวลผลใดสามารถอ้างอิงฐานประโยชน์อันชอบธรรมได้ บริษัทควรจัดทำแบบทดสอบเพื่อพิจารณาความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อประโยชน์อันชอบธรรม และชั่งน้ำหนักระหว่างผลประโยชน์กับสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลก่อน ซึ่งแบบทดสอบดังกล่าวอาจเรียกว่า *การทดสอบสามส่วน (Three-Part Test or Legitimate Interests Assessment: LIA)* โดยสามารถกระทำได้ตามวิธีการดังต่อไปนี้⁵⁵

- (1) การทดสอบวัตถุประสงค์ (Purpose Test): เพื่อระบุและประเมินประโยชน์อันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคล

⁵⁵ Information Commissioner's Office, UK (ICO), 'What is the 'legitimate interests' basis?', ICO < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#article_61f> accessed 13 April 2020

(2) การทดสอบความจำเป็น (Necessity Test): เพื่อประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล

(3) การทดสอบความสมดุล (Balancing Test): เพื่อชั่งน้ำหนักความสำคัญระหว่างประโยชน์อันชอบธรรมกับสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(1) การทดสอบวัตถุประสงค์ (Purpose Test)

ขั้นที่ 1 พยายามตอบคำถามดังต่อไปนี้ เพื่อระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล และประเมินว่าเป็นประโยชน์อันชอบธรรม หรือไม่

- 1) ทำไมถึงต้องประมวลผลข้อมูลส่วนบุคคลนี้
- 2) ประโยชน์ที่จะได้รับการประมวลผลข้อมูลส่วนบุคคลนี้คืออะไร
- 3) มีบุคคลที่สามได้รับประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลนี้หรือไม่
- 4) ประโยชน์ที่ได้รับการประมวลผลข้อมูลส่วนบุคคลมีความสำคัญกับบริษัทหรือไม่
- 5) จะมีผลกระทบอะไรตามมาถ้าไม่สามารถประมวลผลข้อมูลส่วนบุคคลได้
- 6) ผลที่ประสงคต่อเจ้าของข้อมูลส่วนบุคคลจากการประมวลผลข้อมูลส่วนบุคคลนี้คืออะไร
- 7) เป็นการปฏิบัติตามกฎหมายอื่นหรือไม่
- 8) เป็นการปฏิบัติตามแนวทางปฏิบัติของภาคธุรกิจหรือประมวลจริยธรรมหรือไม่
- 9) เป็นการฝ่าฝืนกฎหมายฉบับใดหรือไม่

ข้อสังเกต

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ดังต่อไปนี้ มักจะอ้างอิงฐานประโยชน์อันชอบธรรมได้⁵⁶

- เพื่อป้องกันการฉ้อฉล (Fraud Prevention)

⁵⁶ Information Commissioner's Office, UK (ICO), 'How do we apply legitimate interests in practice?', ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> > accessed 13 April 2020

- เพื่อความมั่นคงปลอดภัยของข้อมูลและเครือข่าย (Network and Information Security)
- เพื่อระบุการกระทำที่อาจเป็นความผิดทางอาญา หรือภัยต่อความมั่นคงสาธารณะ (Indicating Possible Criminal Acts or Threats to Public Security)

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ดังต่อไปนี้ “อาจจะ” อ้างอิงฐานประโยชน์อันชอบธรรม ได้⁵⁷

- เพื่อประมวลผลข้อมูลของลูกค้าจ้าง หรือลูกค้า (Processing Employee or Client Data) หรือ
- การทำการตลาดทางตรง (Direct Marketing)
- การถ่ายโอนข้อมูลภายในเครือ (Intra-Group Administrative Transfers)

(2) การทดสอบความจำเป็น (Necessity Test)

ขั้นที่ 2 บริษัทควรที่จะต้องพิจารณาถึงความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล สำหรับวัตถุประสงค์ที่ได้ระบุไว้ในขั้นที่ 1 ก่อนหน้านี้ โดยการตอบคำถามดังต่อไปนี้

- 1) การประมวลผลข้อมูลส่วนบุคคลนี้จะช่วยให้ บริษัทบรรลุวัตถุประสงค์ข้างต้นได้หรือไม่
- 2) การประมวลผลข้อมูลส่วนบุคคลนี้ได้สัดส่วนกับวัตถุประสงค์ข้างต้นหรือไม่
- 3) บริษัทสามารถบรรลุวัตถุประสงค์ข้างต้น โดยไม่ทำการประมวลผลข้อมูลส่วนบุคคลนี้ หรือทำการประมวลผลข้อมูลส่วนบุคคลให้น้อยลงกว่านี้ได้หรือไม่
- 4) บริษัทสามารถบรรลุวัตถุประสงค์ข้างต้น โดยการประมวลผลข้อมูลส่วนบุคคล ด้วยวิธีการที่ดีกว่า หรือรุกรานสิทธิอันน้อยกว่านี้ได้หรือไม่

⁵⁷ Information Commissioner’s Office, UK (ICO), ‘When can we rely on legitimate interests?’, ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/>> accessed 28 January 2020

(3) การทดสอบความสมดุล (Balancing Test)

ขั้นที่ 3 บริษัทควรที่จะต้องพิจารณาว่า สิทธิขั้นพื้นฐานของเจ้าของข้อมูลสำคัญกว่าประโยชน์อันชอบธรรมที่ได้ระบุไว้ในขั้นที่ 1 ก่อนหน้านี้หรือไม่ โดยมีปัจจัยที่ต้องพิจารณาอย่างน้อยดังต่อไปนี้

1) สภาพของข้อมูลส่วนบุคคล: บริษัทจะต้องพิจารณาถึงความอ่อนไหวของข้อมูลส่วนบุคคลที่จะทำการประมวลผล โดยคำนึงถึงประเด็นตัวอย่างดังนี้

- ข้อมูลดังกล่าว เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษหรือไม่
- ข้อมูลดังกล่าว เป็นข้อมูลส่วนบุคคลที่บุคคลทั่วไปจะเห็นว่าเป็นส่วนตัวเป็นพิเศษ เช่น ข้อมูลทางการเงินหรือไม่
- ข้อมูลดังกล่าว เป็นข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้เยาว์ หรือบุคคลเสมือนหรือไร้ความสามารถหรือไม่
- ข้อมูลดังกล่าว เป็นข้อมูลส่วนบุคคลที่เกี่ยวข้องกับฐานของบุคคลในทางส่วนตัวหรือในทางวิชาชีพหรือไม่

2) ความคาดหวังอย่างสมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคล: บริษัทจะต้องพิจารณาว่า เจ้าของข้อมูลจะสามารถคาดหวังเกี่ยวกับการใช้ข้อมูลส่วนบุคคลในสถานการณ์ต่าง ๆ โดยสามารถคำนึงถึงปัจจัยที่เกี่ยวข้องตัวอย่างดังนี้

- บริษัทมีความสัมพันธ์กับเจ้าของข้อมูลอยู่ก่อนแล้วหรือไม่ และถ้าใช่ เป็นความสัมพันธ์ในรูปแบบใด
- บริษัทใช้ข้อมูลดังกล่าวอย่างไรในอดีต
- บริษัทเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคลโดยตรงหรือไม่
- บริษัทแจ้งอะไรต่อเจ้าของข้อมูลส่วนบุคคลขณะเก็บรวบรวมข้อมูล
- ถ้าบริษัทเก็บรวบรวมข้อมูลจากบุคคลที่สามที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล บริษัทแจ้งอะไรต่อเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลที่ได้รับมา

- ข้อมูลดังกล่าวถูกเก็บมานานเท่าไร และมีข้อเท็จจริงอะไรหรือไม่ ที่จะกระทบต่อความคาดหวังของเจ้าของข้อมูลส่วนบุคคล
- วัตถุประสงค์หรือวิธีการในการประมวลผลข้อมูลของบริษัทเป็นที่ประจักษ์ และเข้าใจโดยทั่วไปหรือไม่
- บริษัทมีแผนการดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล รูปแบบใหม่หรือไม่
- บริษัทมีหลักฐานเกี่ยวกับความคาดหวังหรือไม่
- มีปัจจัยอื่น หรือข้อเท็จจริงอื่นที่จะทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถ คาดหมายถึงการประมวลผลข้อมูลนี้หรือไม่

อนึ่ง บริษัทไม่จำเป็นจะต้องตอบคำถามข้างต้นได้ทุกคำถาม แต่ถ้าหากไม่สามารถ หาคำตอบของคำถามข้างต้นได้ทันที บริษัทอาจจะต้องค้นคว้าเพิ่มเติมเพื่อหาข้อสรุป

3) ผลกระทบที่น่าจะเกิดขึ้นและมาตรการป้องกัน: บริษัทจะต้องพิจารณาว่าจะมีผลกระทบอะไรที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในครั้งนี้ ถ้ามีความเสี่ยงสูง ที่จะกระทบสิทธิพื้นฐานของเจ้าของข้อมูลส่วนบุคคล บริษัทควรทำการประเมินผลกระทบ ด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เพิ่ม แต่ถ้าบริษัทตัดสินใจว่า DPIA ไม่มีความจำเป็น บริษัทควรคำนึงว่าการประมวลผลข้อมูลครั้งนี้จะส่งผลกระทบทำให้เกิดหรือก่อให้เกิดสิ่งตามมาอย่างไรบ้าง เช่น

- สิ่งที่ขัดขวางในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (ไม่จำกัดเพียงสิทธิใน ความเป็นส่วนตัว)
- สิ่งที่ขัดขวางเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงบริการหรือโอกาส
- การสูญเสียการควบคุมเกี่ยวกับการใช้ข้อมูลส่วนบุคคลในอนาคต
- อันตรายทางกายภาพ
- ความเสียหายทางการเงิน การถูกขโมยตัวตน (Identity Theft) หรือการฉ้อโกง
- การเสียโอกาสทางเศรษฐกิจหรือทางสังคมที่สำคัญใด ๆ (เช่น การถูกเหยียด เชื้อชาติ การสูญเสียชื่อเสียง และการถูกเปิดเผยความลับ เป็นต้น)

- ความเหมาะสมและเพียงพอของมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล
- การอนุญาตให้เจ้าของข้อมูลส่วนบุคคลปฏิเสธหรือถอนตัว (opt-out)

ถ้าบริษัทสามารถระบุความเสี่ยงข้างต้นได้แล้ว บริษัทจะต้องสามารถระบุประโยชน์อันชอบธรรมที่สำคัญอย่างยิ่งที่สามารถทำให้เกิดความสมดุลระหว่างผลกระทบกับประโยชน์ที่จะได้รับ ในแง่ที่ว่าได้ประโยชน์มากกว่าผลกระทบ และการที่บริษัทจัดให้มีมาตรการป้องกัน หรือรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้น อาจเป็นการลดผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลได้ อันทำให้น้ำหนักในส่วนของการกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคลลดลงตามไปด้วย

ข้อแนะนำ บริษัทควรทำการบันทึกการทำและผลของ Legitimate Interest Assessment (LIA) ไว้ เพื่อใช้เป็นหลักฐานสนับสนุนว่าการใช้ดุลพินิจของบริษัทได้กระทำไปโดยมีขั้นตอนการทดสอบการใช้ดุลพินิจ ในกรณีที่มีการตรวจสอบย้อนหลังหรือเกิดข้อพิพาทเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลขึ้น

ข้อสังเกต สิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลของผู้เยาว์มักจะถูกพิจารณาว่าเป็นข้อมูลส่วนบุคคลที่มีความสำคัญและมักจะได้รับความคุ้มครองเป็นพิเศษ⁵⁸

ตัวอย่างของการประมวลผลบนฐานผลประโยชน์อันชอบธรรม

การยืนยันตัวตนผู้มุ่งหวังเอาประกันภัย - บริษัทอาจดำเนินการประมวลผลข้อมูลส่วนบุคคลตามแนวปฏิบัติของตนเพื่อตรวจสอบและยืนยันตัวตนของผู้มุ่งหวังเอาประกันภัยกับบริษัท ในกรณีนี้ผลประโยชน์ของบริษัท คือ ทำให้บริษัทสามารถระบุตัวลูกค้าและให้บริการได้อย่างถูกต้อง ลดและป้องกันการฉ้อโกง ที่เกิดจากการสวมตัวตนของลูกค้าได้อย่างมีประสิทธิภาพ ซึ่งถือว่าเป็นประโยชน์อันชอบธรรม สำหรับบริษัท และบริษัทอื่น ๆ ในธุรกิจประกันวินาศภัยด้วย ทั้งนี้ การดำเนินการดังกล่าวต้องมีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ดี ตลอดจนไม่นำข้อมูลส่วนบุคคลดังกล่าวไปประมวลผลเพื่อวัตถุประสงค์อื่น ซึ่งอาจทำให้กระทบสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของลูกค้ามากเกินไป ดังนั้น หากบริษัทประมวลผลข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อพิสูจน์ยืนยันตัวตนตามข้างต้น ย่อมเป็นการกระทำที่ได้สัดส่วน และไม่กระทบสิทธิของเจ้าของข้อมูลส่วนบุคคล และสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้

กรณีที่บริษัทมีการดำเนินการจัดให้ลูกค้าแสดงตน (KYC) และตรวจสอบเพื่อทราบข้อเท็จจริงของลูกค้า (CDD) ตามที่ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน กำหนดนั้น บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมายในการดำเนินการดังกล่าวได้

⁵⁸ ข้อ 6(1)(f) GDPR

ข้อมูลการทำงานของพนักงาน - บริษัทเก็บรวบรวมข้อมูลเพื่อการจ้างงานอินเทอร์เน็ตของพนักงานเพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรสารสนเทศของบริษัทไปเพื่อการส่วนตัวมากเกินไป ข้อมูลเหล่านี้ เช่น ข้อมูลคุกกี้ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด ส่วนใหญ่แล้วถูกประมวลผลไปโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน หรือมิได้แจ้งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน ในกรณีนี้ แม้บริษัทจะมีผลประโยชน์อันชอบธรรมในฐานะนายจ้าง แต่การเก็บรวบรวมข้อมูลดังกล่าวอาจขัดกับสิทธิความเป็นส่วนตัวของพนักงานมากเกินไป และไม่ได้สัดส่วน เพราะยังมีวิธีการอื่นที่ละเมิดสิทธิความเป็นส่วนตัวของพนักงานน้อยกว่าการเก็บรวบรวมข้อมูลโดยการเฝ้าระวัง เช่น จำกัดการเข้าถึงเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น กรณีนี้บริษัทจึงไม่สามารถอ้างอิงฐานผลประโยชน์อันชอบธรรม ในการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงานได้

การแจ้งห้ามโทรศัพท์ (Do-Not-Call) - ในกรณีที่บุคคลได้ร้องขอไม่ให้โทรศัพท์มาเสนอขายผลิตภัณฑ์ (Telesale) อีกนั้น บริษัทอาจอ้างอิงฐานผลประโยชน์อันชอบธรรมในการที่จะเก็บข้อมูลชื่อและช่องทางการติดต่อลูกค้ารายนั้นไว้เพื่อไม่ให้เกิดโทรไปเสนอขายอีกในอนาคตได้ ทั้งนี้ เนื่องจาก Do-Not-Call List นี้เป็นการดำเนินการก็เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ดังนั้น การประมวลผลข้อมูลส่วนบุคคลในกรณีนี้จึงไม่ได้เป็นการกระหนาบสิทธิของเจ้าของข้อมูลส่วนบุคคลมากเกินไป

การแบ่งปันข้อมูล - กรณีการฉ้อฉลประกันภัย ภาคธุรกิจประกันภัยอาจแบ่งปันข้อมูลการรับประกันภัย รวมถึงข้อมูลส่วนบุคคลที่จำเป็น เพื่อวัตถุประสงค์ในการยับยั้ง ป้องกัน ตรวจสอบ รายงาน และบรรเทาความเสียหายจากการฉ้อฉลประกันภัย ซึ่งจะส่งผลให้เบี้ยประกันภัยโดยรวมมีความเหมาะสมตามความเสี่ยงภัยที่แท้จริงมากยิ่งขึ้น และเป็นประโยชน์สาธารณะต่อผู้เอาประกันภัย

อย่างไรก็ตาม การแบ่งปันข้อมูลนี้ควรต้องดำเนินการโดยมีมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เพียงพอและเหมาะสม และมีการทบทวนมาตรการการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เช่น ขั้นตอนการตรวจสอบความถูกต้องของข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูล ระบบการตรวจสอบการใช้ดุลพินิจที่ไม่เป็นธรรม เพราะข้อมูลเหล่านี้ อาจรวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ประวัติอาชญากรรม ประวัติสุขภาพ เป็นต้น ทั้งนี้ ภาคธุรกิจควรกำหนดมาตรฐานร่วมกับสำนักงาน คปภ. ในการดำเนินการดังกล่าว

การเสนอขายผลิตภัณฑ์แก่ลูกค้าปัจจุบัน/เก่า - การเสนอขายในกรณีนี้อาจใช้ฐานผลประโยชน์อันชอบธรรมได้ เมื่อบริษัทได้มีการประเมินผลกระทบเพื่อสนับสนุนดุลพินิจของบริษัทแล้ว ทั้งนี้ การเสนอขายผลิตภัณฑ์ของบุคคลที่สามแก่ลูกค้าของบริษัทไม่สามารถอ้างอิงหลักการของฐานผลประโยชน์อันชอบธรรม

5.1.7 ฐานจตหมายเหตุ/ วิจัย/ สถิติ

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (1) ได้กำหนด ฐานจตหมายเหตุ/ วิจัย/ สถิติ ขึ้นมา เป็นฐานในการประมวลผลข้อมูลส่วนบุคคลเป็นพิเศษ แตกต่างไปจากกฎหมายของประเทศอื่น รวมถึง GDPR โดยกฎหมายอนุญาตให้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการประมวลผลข้อมูลส่วนบุคคลได้ เพื่อวัตถุประสงค์ ดังต่อไปนี้ได้

- 1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจตหมายเหตุ เพื่อประโยชน์สาธารณะ หรือ
- 2) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ และ
- 3) จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (ตามที่คณะกรรมการประกาศกำหนด)

ข้อสังเกต

- คำว่า “เพื่อประโยชน์สาธารณะ” มีไว้สำหรับการประมวลผลข้อมูลส่วนบุคคลจำกัดเพียง เพื่อการจัดทำ “เอกสารประวัติศาสตร์” หรือ “จตหมายเหตุ” เท่านั้น
- การประมวลผลข้อมูลส่วนบุคคลที่ไม่ใช่เพื่อประโยชน์สาธารณะ เช่น เพื่อประโยชน์ในการดำเนินธุรกิจ แม้ทำไปเพื่อจัดทำ “เอกสารประวัติศาสตร์” หรือ “จตหมายเหตุ” ก็ไม่สามารถอ้างอิงฐานจตหมายเหตุ/ วิจัย/ สถิตินี้ได้
- วัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ในกรณีนี้ไม่ถูกจำกัดให้ต้องทำ “เพื่อประโยชน์สาธารณะ”
- ในเรื่องการจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลนั้น เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ระบุว่า “(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจตหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด” ดังนั้น อาจทำให้เกิดการตีความได้ 2 กรณี คือ

(1) การจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลกำหนดไว้เพียงสำหรับการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการศึกษาวิจัยหรือสถิติเท่านั้น ไม่รวมถึงกรณีการประมวลผลข้อมูลส่วนบุคคลเพื่อบรรลุ

วัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือ

(2) การจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลกำหนดไว้สำหรับการประมวลผลข้อมูลส่วนบุคคลทั้ง 2 กรณีคือ เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ และการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการศึกษาวิจัย หรือสถิติ

หากพิจารณาตามเจตนารมณ์ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ อาจพิจารณาได้ว่าการจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลนั้นใช้สำหรับการประมวลผลข้อมูลส่วนบุคคลทั้ง 2 กรณี ทั้งนี้ การตีความ และแนวทางปฏิบัติให้เป็นไปตามกฎหมายลำดับรอง

ตัวอย่าง บริษัทอาจประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ในการทำการศึกษาวิจัยหรือสถิติเกี่ยวกับตลาดหรือการพัฒนาผลิตภัณฑ์ใหม่ ๆ หรือการหา กลุ่มลูกค้าใหม่ (New Target Group) ได้โดยที่บริษัทต้องจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ข้อควรระวัง การประมวลผลข้อมูลส่วนบุคคลเพื่อการศึกษวิจัยหรือสถิติเกี่ยวกับตลาดในกรณีนี้ มีความหมายในลักษณะเป็นการทำการศึกษวิจัยตลาดเพื่อใช้ภายในบริษัท (Internal Market Research/ Intelligent) ไม่ใช่การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดหรือทำกิจกรรมส่งเสริมการขาย ซึ่งมีลักษณะเป็นการกระทำที่ต้องมีการติดต่อสื่อสารระหว่างบริษัทกับลูกค้าที่เป็นเจ้าของข้อมูลส่วนบุคคล

5.2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ตามที่ได้อธิบายไว้แล้วเบื้องต้นเกี่ยวกับนิยามของคำว่า “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” (Sensitive Personal Data) ที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ได้กำหนดบทนิยามไว้เป็นการเฉพาะ มีเพียงการกำหนดในเรื่องฐานการประมวลผลข้อมูลส่วนบุคคลบางประเภทไว้เป็นพิเศษในมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งข้อมูลส่วนบุคคลที่ถูกกำหนดเหล่านั้น ล้วนมีลักษณะเป็นข้อมูลที่สามารถก่อให้เกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคลได้มากกว่าข้อมูลส่วนบุคคลประเภทอื่น ๆ เช่น การนำไปสู่การเลือกปฏิบัติ ซึ่งแนวทางปฏิบัตินี้จะเรียกข้อมูลส่วนบุคคลเหล่านี้ว่า “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หรือ “Sensitive Personal Data” หรือ “Special Category Data” โดยข้อมูลดังกล่าว ได้แก่

1. ข้อมูลส่วนบุคคลเกี่ยวกับ**เชื้อชาติ** หรือเผ่าพันธุ์ เช่น คำถามเกี่ยวกับเชื้อชาติบนใบสมัครงาน
2. ข้อมูลส่วนบุคคลเกี่ยวกับความเห็นทางการเมือง
3. ข้อมูลส่วนบุคคลเกี่ยวกับความเชื่อในลัทธิ ศาสนาหรือปรัชญา
4. ข้อมูลส่วนบุคคลเกี่ยวกับความพิการ เช่น คำถามเรื่องความพิการในใบสมัครงาน
5. ข้อมูลส่วนบุคคลเกี่ยวกับพฤติกรรมทางเพศ
6. ข้อมูลสภาพแรงงาน
7. **ข้อมูลสุขภาพ** เช่น ประวัติสุขภาพ, แบบตอบคำถามสุขภาพ, คำถามถึงโรคประจำตัว
8. ข้อมูลพันธุกรรม
9. ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา และข้อมูลจำลองลายนิ้วมือ
10. ประวัติอาชญากรรม
11. ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการกำหนด

ข้อควรระวัง

เมื่อ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้ทั้งฉบับแล้ว บริษัทต้องคอยติดตามว่า คณะกรรมการจะประกาศกำหนดข้อมูลส่วนบุคคลใดให้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 26 เพิ่มเติม

ดังที่กล่าวข้างต้น การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะมีฐานโดยชอบด้วยกฎหมายที่ต่างกับการประมวลผลข้อมูลส่วนบุคคลทั่วไป (มาตรา 24) ซึ่งฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวสามารถแบ่งได้ 10 ฐาน ดังต่อไปนี้

1. ฐานความยินยอม (โดยชัดแจ้ง)
2. ฐานประโยชน์ที่สำคัญต่อชีวิต
3. ฐานเพื่อการดำเนินการของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร
4. ฐานข้อมูลที่เปิดเผยโดยสาธารณะโดยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

5. ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับสิทธิเรียกร้อง
6. ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคม
7. ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับเวชศาสตร์ป้องกัน หรืออาชีวศาสตร์
8. ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข
9. ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ
10. ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ

5.2.1 ฐานความยินยอม⁵⁹

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลอ้างอิงฐานความยินยอม เป็นหนึ่งในฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยที่ความยินยอมในกรณีนี้จะต้องเป็น**ความยินยอมโดยชัดแจ้ง (Explicit Consent)** ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26

เงื่อนไขเกี่ยวกับความยินยอม

หากพิจารณาเปรียบเทียบเงื่อนไขเกี่ยวกับฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคลทั่วไป กับเงื่อนไขฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลแล้ว จะสังเกตได้ว่า มาตรา 26 กำหนดให้ต้อง “ได้รับความยินยอมโดยชัดแจ้ง” สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ในขณะที่ มาตรา 19 และมาตรา 24 ซึ่งเป็นหลักการประมวลผลข้อมูลส่วนบุคคลทั่วไป ไม่ได้มีการกำหนดลักษณะของความยินยอมที่จะต้องได้รับไว้ โดยเฉพาะ มีแต่เพียงกำหนดว่า “การขอความยินยอมต้องทำโดยชัดแจ้ง” เท่านั้น

ทั้งนี้ จากบทบัญญัติและรายละเอียดดังกล่าวข้างต้น สามารถสรุปได้ดังนี้

⁵⁹ Information Commissioner’s Office, UK (ICO), ‘What are the conditions for processing?’, ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/>> accessed 13 April 2020

ประเด็น	บทบัญญัติที่เกี่ยวข้อง	ข้อมูลส่วนบุคคลทั่วไป Personal Data	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว Sensitive Personal Data
การขอความยินยอม	มาตรา 19	หลักในเรื่องการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลไม่ว่าจะเป็นการขอความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลทั่วไป หรือการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น มีเงื่อนไขในการขอความยินยอมที่เหมือนกันตามมาตรา 19 คือ 1. ขอความยินยอม ก่อน หรือขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล 2. การขอความยินยอมต้องกระทำโดยชัดแจ้ง 3. การขอความยินยอมต้องกระทำเป็นลายลักษณ์อักษร หรือทางอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจทำโดยวิธีดังกล่าวได้ 4. ต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล 5. การขอความยินยอมต้องแยกส่วนออกจากข้อความอื่น 6. ข้อความขอความยินยอมจะต้องใช้ภาษาที่อ่านง่าย เข้าใจได้ ไม่หลอกลวง และเข้าถึงได้ง่าย 7. คำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคล (ในการเข้าทำสัญญา หรือการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อการประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นเกี่ยวกับการเข้าทำสัญญา หรือการให้ความยินยอมนั้น ๆ)	
การได้รับความยินยอม หรือการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล	มาตรา 24, มาตรา 26	ไม่มีการกำหนดเงื่อนไขเกี่ยวกับลักษณะของ ความยินยอมที่จะต้องได้รับ ดังนั้น ความยินยอมที่ได้รับมานั้นจึงไม่ถูกกำหนดรูปแบบหรือลักษณะพิเศษ แต่ในทางปฏิบัติ เมื่อการขอความยินยอมกำหนดให้ต้องทำเป็นลายลักษณ์อักษร หรือทางอิเล็กทรอนิกส์แล้ว ความยินยอมที่เจ้าของข้อมูลส่วนบุคคลจะให้กับบริษัท ก็ควรอยู่ในรูปแบบเดียวกัน ทั้งนี้ เพื่อประโยชน์ในการติดตามการประมวลผล และเพื่อเป็นหลักฐานในการขอและได้รับความยินยอม	มีการกำหนดว่าต้อง “<u>ได้รับความยินยอมโดยชัดแจ้ง</u>” ซึ่งตรงกับภาษาอังกฤษว่า “Explicit Consent” เนื่องจากปัจจุบัน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลไม่ได้กำหนดคำอธิบาย หรือกำหนดลักษณะของความยินยอมโดยชัดแจ้ง แต่จากกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลสากล มีแนวทางการพิจารณาลักษณะของความยินยอมโดยชัดแจ้ง ดังนี้ • มีลักษณะเป็นประโยชน์ที่ยืนยันความประสงค์ที่จะให้ยินยอมอย่างชัดเจน ไม่ว่าจะเป็นกระทำด้วยวาจาหรือลายลักษณ์อักษร แต่จะไม่อาจถือเอาการกระทำอื่นเป็นความยินยอมโดยชัดแจ้งได้

ประเด็น	บทบัญญัติที่เกี่ยวข้อง	ข้อมูลส่วนบุคคลทั่วไป Personal Data	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว Sensitive Personal Data
			• ประโยคที่ยืนยันความประสงค์ที่จะให้ยินยอมดังกล่าว ยังควรต้องระบุถึงรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลที่กฎหมายกำหนดให้ขอความยินยอมโดยชัดแจ้งอีกด้วย⁶⁰ กล่าวคือ ลักษณะของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 • ควรแยกออกจากการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลอื่น

5.2.2 ฐานประโยชน์ที่สำคัญต่อชีวิต⁶¹ (Vital Interest)

ในส่วนของการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานประโยชน์ที่สำคัญต่อชีวิต การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะต้องเป็นไปเพื่อวัตถุประสงค์ดังต่อไปนี้ โดยที่เจ้าของข้อมูลส่วนบุคคลไม่อยู่ในสถานะที่สามารถให้ความยินยอมได้ เท่านั้น

- ป้องกันหรือระงับอันตรายต่อชีวิต
- ป้องกันหรือระงับอันตรายต่อร่างกาย
- ป้องกันหรือระงับอันตรายต่อสุขภาพของบุคคล

⁶⁰ Information Commissioner's Office, UK (ICO), 'What is valid consent?', ICO <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/>> accessed 14 April 2020

⁶¹ Information Commissioner's Office, UK (ICO), 'What are the conditions for processing?', ICO <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/>> accessed 15 April 2020

ข้อสังเกต

- “เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้” หมายความว่า กรณีที่เจ้าของข้อมูลส่วนบุคคลไม่อยู่ในสถานะที่สามารถให้ความยินยอมได้ ซึ่งรวมถึงทั้งทางกายภาพและในทางกฎหมาย เช่น เป็นคนที่ศาลสั่งให้เป็นคนไร้ความสามารถ เป็นต้น
- ประโยชน์ที่สำคัญต่อชีวิตในที่นี้ จะต้องเกี่ยวกับเรื่องความเป็นความตายเท่านั้น เรื่องอื่น เช่น การเบิกค่าใช้จ่ายในการรักษาที่เป็นการผ่าตัดรักษาชีวิต ไม่ถือเป็นเรื่องความเป็นความตายและไม่สามารถอ้างอิงฐานนี้ได้

ทั้งนี้ คณะกรรมการร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลได้มีการให้ข้อสังเกตไว้ว่า “... ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตามนั้น หมายความว่าข้อมูลเกี่ยวกับชีวิต ร่างกาย หรือสุขภาพทุกประเภท ซึ่งรวมกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อการบริการทางการแพทย์ กรณีบริจาคอวัยวะ การบริจาคร่างกาย และการปฏิบัติตามเจตนาไม่ประสงค์จะรับบริการสาธารณสุขที่เป็นไปเพียงเพื่อยื้อการตายในวาระสุดท้ายของชีวิตของบุคคล หรือเพื่อยุติการทรมานจากการเจ็บป่วยด้วย หรือกรณีร่างมาตรา 26 (1) [เลขมาตราเดิม] ควรตีความให้ครอบคลุมถึงกรณีการบริการทางการแพทย์ที่เป็นประโยชน์กับเจ้าของข้อมูลส่วนบุคคลที่อยู่ในสถานะไม่อาจให้ความยินยอมได้ทุกกรณี รวมถึงกรณีไม่เร่งด่วนด้วย โดยไม่ใช่เพื่อป้องกันหรือระงับอันตรายที่ใกล้จะถึงเท่านั้น...”⁶²

5.2.3 ฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไร⁶³

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทสามารถอ้างอิงฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรได้⁶⁴ โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยข้อยกเว้นในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ มีเงื่อนไขดังต่อไปนี้

⁶² ข้อสังเกตคณะกรรมการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล,
https://ictlawcenter.etda.or.th/de_laws/download_file/5_Notice_Draft-DP.pdf

⁶³ Information Commissioner’s Office, UK (ICO), ‘What are the conditions for processing?’, ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/> accessed 15 April 2020

⁶⁴ มาตรา 26 (2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- (1) เป็นมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสภาพแรงงาน เช่น พรรคการเมือง วัด หรือมูลนิธิชัยพัฒนา เป็นต้น
- (2) การประมวลผลข้อมูลมีความอ่อนไหวดังกล่าวเป็นส่วนหนึ่งของการดำเนินกิจกรรมโดยชอบด้วยกฎหมาย
- (3) เป็นการประมวลผลข้อมูลของสมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับองค์กรที่ไม่แสวงหากำไร (เช่น ผู้บริจาค หรือผู้รับประโยชน์) แต่ไม่รวมถึงลูกจ้าง หรือพนักงานขององค์กร หรือผู้ที่อาจจะเป็นสมาชิกในอนาคต
- (4) มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เช่น การจำกัดการเข้าถึงข้อมูล การแฝงข้อมูล การที่มีระยะเวลาเก็บรักษาข้อมูลที่สั้น เป็นต้น
- (5) ไม่เปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

จากเงื่อนไขข้างต้น จะเห็นได้ว่า สมาคมประกันวินาศภัยไทยไม่ได้เข้าเงื่อนไขข้อยกเว้นดังกล่าว เนื่องจากไม่ได้เป็นสมาคมที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสภาพแรงงาน ดังนั้น หากบริษัทจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อสมาคม บริษัท จะต้องอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามที่กำหนดในมาตรา 26

5.2.4 ฐานข้อมูลที่เปิดเผยต่อสาธารณะ⁶⁵

บริษัทสามารถอ้างอิงฐานข้อมูลที่เปิดเผยต่อสาธารณะในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ โดยไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลตามที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ เงื่อนไขสำคัญในการอ้างอิงฐานการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ คือ ข้อมูลที่มีความอ่อนไหวที่ถูกประมวลผลนั้น ต้องเป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคลเอง กล่าวคือ เจ้าของข้อมูลส่วนบุคคลเป็นคนเปิดเผยข้อมูลนั้นต่อสาธารณะด้วยตัวเอง

หากบริษัท ต้องการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานการประมวลผลนี้ บริษัทควรที่จะพิจารณาคำถามต่อไปนี้

⁶⁵ มาตรา 26 (3) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- ข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ ถูกเปิดเผยต่อสาธารณะหรือไม่? ประชาชนทั่วไปสามารถเข้าถึงข้อมูลนี้ได้จริงหรือไม่ในทางปฏิบัติ
- ใครเป็นผู้เปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ และถูกเปิดเผยต่อสาธารณะในบริบทใด เช่น การโพสต์ลงโซเชียลมีเดีย การเขียนหนังสือ การหาเสียงเลือกตั้ง หรือการให้สัมภาษณ์สื่อ
- เจ้าของข้อมูลส่วนบุคคลได้กระทำการโดยมีเจตนาเพื่อเปิดเผยข้อมูลต่อสาธารณะหรือไม่? เจ้าของข้อมูลส่วนบุคคลคนนั้นเข้าใจถึงผลของการกระทำที่เป็นการเปิดเผยข้อมูลต่อสาธารณะหรือไม่

ในการอ้างอิงฐานข้อมูลที่ถูกเปิดเผยต่อสาธารณะนี้ บริษัทจะต้องมั่นใจอย่างมากว่า เจ้าของข้อมูลส่วนบุคคลมีเจตนาที่จะเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวด้วยตัวเอง เพราะเป็นการยากในการพิสูจน์ได้ว่าการเปิดเผยข้อมูลส่วนบุคคลต่อสาธารณะนั้น เป็นไปโดยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง

- เว็บไซต์ของพรรคการเมือง เอ แสดงข้อมูลการเป็นสมาชิกของนาย ก. ในหน้าหลักของเว็บไซต์พรรค เนื่องจากเว็บไซต์ของพรรคถูกขโมยข้อมูลและนำข้อมูลดังกล่าวมาเปิดเผยต่อสาธารณะ เช่นนี้ย่อมเป็นที่เข้าใจได้ว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลความเห็นทางการเมืองนี้ ไม่ได้ถูกเปิดเผยโดยตัวของนาย ก. เจ้าของข้อมูลส่วนบุคคลเอง
- นาย ข. โพสต์ข้อความลงในเฟซบุ๊ก (Facebook) โดยตั้งค่าความเป็นส่วนตัวของโพสต์เป็น “สาธารณะ” ว่าตนกำลังติดเชื้อไวรัส COVID – 19 เช่นนี้ เนื่องจากเฟซบุ๊กอนุญาตให้ผู้ใช้สามารถตั้งค่าความเป็นส่วนตัวได้ทุกโพสต์ และนาย ข. เลือกที่จะตั้งค่าความเป็นส่วนตัวเป็น “สาธารณะ” ดังนั้น จึงอาจเป็นกรณีที่นาย ข. เจ้าของข้อมูลส่วนบุคคลเจตนาเปิดเผยว่าตนติดเชื้อไวรัส COVID – 19 สู่สาธารณะด้วยความยินยอมโดยชัดแจ้งของนาย ข. เอง
- นาย ค. ตั้งชื่อบัญชีของตนว่า “นาย ค. คนเลียดบวก” โดยที่นาย ค. ตั้งค่าให้บัญชีของตนให้เป็นบุคคลสาธารณะ เช่นนี้ อาจถือได้ว่า ข้อมูลสุขภาพที่เกี่ยวกับโรคเอดส์ของนาย ค. ถูกเปิดเผยให้เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยตัวเจ้าของข้อมูลส่วนบุคคลเองแล้ว

5.2.5 ฐานความจำเป็นเพื่อก่อตั้งสิทธิเรียกร้อง⁶⁶

บริษัทสามารถอ้างถึงฐานความจำเป็นเพื่อก่อตั้งสิทธิเรียกร้อง⁶⁷ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อการก่อตั้งสิทธิเรียกร้องได้ เนื่องจากเป็นข้อยกเว้นของเงื่อนไขในการได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยมีวัตถุประสงค์เพื่อดำเนินการ ดังต่อไปนี้

- (1) การก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- (2) การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
- (3) การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ซึ่งมีตัวอย่างกิจกรรม ดังนี้

- (1) การจ้างบริษัทกฎหมายเพื่อดำเนินการตามสิทธิเรียกร้อง
- (2) การดำเนินการเกี่ยวกับการบังคับคดี
- (3) การดำเนินการเกี่ยวกับการรับช่วงสิทธิของผู้เอาประกันภัย

ตัวอย่าง

- ลูกจ้างของบริษัทบาดเจ็บจากอุบัติเหตุในที่ทำงานและฟ้องเรียกค่าเสียหายจากบริษัท
ดังนี้ บริษัทสามารถนำข้อมูลรายละเอียดเกี่ยวกับบาดเจ็บและการรักษาของลูกจ้าง (ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว) มาประมวลผลข้อมูลเพื่อเตรียมข้อต่อสู้หรือคำให้การในชั้นศาล
- ผู้เอาประกันภัยสุขภาพ ได้รับอุบัติเหตุและฟ้องเรียกค่าสินไหมทดแทนจากบริษัท โดยที่ผู้เอาประกันภัยคนนี้มีประวัติฉ้อโกงประกันภัยมาอยู่ก่อนแล้ว บริษัทสามารถนำข้อมูลสุขภาพและประวัติการกระทำความผิดของผู้เอาประกันภัย มาประมวลผลข้อมูลเพื่อเตรียมข้อต่อสู้ในคำให้การ หรือข้อเรียกร้องในคำฟ้องแย้งได้ (หากมี)

⁶⁶ Information Commissioner's Office, UK (ICO), 'What are the conditions for processing?', ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/> > accessed 15 April 2020

⁶⁷ มาตรา 26 (4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

5.2.6 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคม (Employment, Social Security and Social Protection Law)

บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมาย⁶⁸ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้โดยไม่ต้องขอและได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพราะความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคมนี้ เป็นข้อยกเว้นในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องดำเนินการตามเงื่อนไข ดังนี้

- (1) บริษัทต้องมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย กล่าวคือ เป็นกรณีที่กฎหมายกำหนดหน้าที่ให้บริษัทต้องประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และอาจรวมถึงกรณีมีประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติที่กำหนดโดยหน่วยงานของรัฐที่มีอำนาจด้วย
- (2) บริษัททำการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้
 - การคุ้มครองแรงงาน
 - การประกันสังคม
 - หลักประกันสุขภาพแห่งชาติ
 - สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย
 - การคุ้มครองผู้ประสบภัยจากรถ
 - การคุ้มครองทางสังคม
- (3) การประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไว้นั้นเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของบริษัท หรือเจ้าของข้อมูลส่วนบุคคล
- (4) บริษัทได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

⁶⁸ มาตรา 26 (5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่าง

ในกรณีที่บริษัทมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวของผู้เอาประกันภัยรถยนต์ เช่น ประวัติการรักษาของผู้เอาประกันภัยที่ประสบอุบัติเหตุ ให้กับบริษัท กลางคุ้มครองผู้ประสบภัยจากรถ จำกัด เพื่อใช้เป็นหลักฐานประกอบการพิจารณาจ่ายค่าสินไหมทดแทนที่เป็นส่วนเกินจากค่าเสียหายเบื้องต้น ภายใต้พระราชบัญญัติคุ้มครองผู้ประสบภัยจากรถ พ.ศ. 2535

5.2.7 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับเวชศาสตร์ป้องกัน หรืออาชีวศาสตร์ (Health or Social Care)

บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมาย⁶⁹ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ โดยบริษัทไม่จำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากเป็นข้อยกเว้นในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องดำเนินการตามเงื่อนไข ดังนี้

- (1) บริษัทต้องมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย กล่าวคือ เป็นกรณีที่กฎหมายกำหนดหน้าที่ให้บริษัทต้องประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และอาจรวมถึงกรณีมีประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติที่กำหนดโดยหน่วยงานของรัฐที่มีอำนาจด้วย
- (2) บริษัททำการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้
 - เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์
 - การประเมินความสามารถในการทำงานของลูกจ้าง
 - การวินิจฉัยโรคทางการแพทย์
 - การให้บริการด้านสุขภาพหรือด้านสังคม
 - การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

⁶⁹ มาตรา 26 (5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- (3) กรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

5.2.8 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข (Public Health)

บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมาย⁷⁰ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ โดยบริษัทไม่จำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากการประมวลผลข้อมูลส่วนบุคคลโดยการอ้างอิงฐานนี้เป็นข้อยกเว้นในเรื่องการได้รับความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องดำเนินการตามเงื่อนไข ดังนี้

- (1) บริษัทต้องมี**ความจำเป็น**ในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย กล่าวคือ เป็นกรณีที่กฎหมายกำหนดหน้าที่ให้บริษัทต้องประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และอาจรวมถึงกรณีมีประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติที่กำหนดโดยหน่วยงานของรัฐที่มีอำนาจด้วย
- (2) บริษัททำการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้
 - ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือ
 - การควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์
- (3) บริษัทได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

⁷⁰ มาตรา 26 (5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

5.2.9 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ (Archiving, Research and Statistics)

บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมาย⁷¹ ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ โดยที่ไม่จำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากการประมวลผลข้อมูลส่วนบุคคลโดยการอ้างอิงฐานนี้เป็นข้อยกเว้นในเรื่องการได้รับความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องดำเนินการตามเงื่อนไข ดังนี้

- (1) บริษัทต้องมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย กล่าวคือ เป็นกรณีที่กฎหมายกำหนดหน้าที่ให้บริษัทต้องประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และอาจรวมถึงกรณีมีประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติที่กำหนดโดยหน่วยงานของรัฐที่มีอำนาจด้วย
- (2) บริษัทต้องทำการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น
- (3) บริษัทต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และ
- (4) บริษัทได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

ข้อสังเกต

Information Commissioner's Office ของประเทศสหราชอาณาจักร ให้ความเห็นว่าการศึกษาทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นนี้ ครอบคลุมทั้งภาครัฐและเอกชน ดังนั้นการศึกษาทางวิทยาศาสตร์ที่มีลักษณะทางพาณิชย์จึงอาจจะเข้าลักษณะของฐานการประมวลผลข้อมูลนี้ได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องสามารถแสดงให้เห็นว่า การศึกษาดังกล่าวนั้นได้ใช้วิธีการทางวิทยาศาสตร์และมีประโยชน์ต่อสาธารณะได้ด้วย เช่น การประมวลผลข้อมูลส่วนบุคคลที่ได้รับจากบริษัท เพื่อจัดทำเป็นสถิติประเมินแนวโน้มความเป็นไปของตลาดประกันวินาศภัยโดยรวม หรือตลาดประกันวินาศภัยส่วนบุคคล ในอนาคต สถิติเช่นนี้นอกจากจะเป็นประโยชน์ในทางพาณิชย์แก่บริษัท ในแง่ที่จะช่วยคาดการณ์ความเป็นไปของผลิตภัณฑ์ประกันวินาศภัยแต่ละประเภทแล้ว ยังเป็นประโยชน์แก่ สำนักงาน คปภ. ในการประเมินแนวโน้มของตลาดประกันวินาศภัยในอนาคตเพื่อกำหนดแนวนโยบายของสำนักงาน คปภ. ต่อไป

⁷¹ มาตรา 26 (5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

5.2.10 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ (Substantial Public Interest)

บริษัทสามารถอ้างอิงฐานหน้าที่ตามกฎหมาย⁷² ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวได้ โดยไม่จำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากการประมวลผลข้อมูลส่วนบุคคลโดยการอ้างอิงฐานนี้เป็นข้อยกเว้นในเรื่องการได้รับความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ บริษัทจะต้องดำเนินการตามเงื่อนไข ดังนี้

- (1) บริษัทต้องมี**ความจำเป็น**ในการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย กล่าวคือ เป็นกรณีที่กฎหมายกำหนดหน้าที่ให้บริษัทต้องประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และอาจรวมถึงกรณีมีประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติที่กำหนดโดยหน่วยงานของรัฐที่มีอำนาจด้วย
- (2) บริษัททำการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว เพื่อให้บรรลุวัตถุประสงค์ **ประโยชน์สาธารณะที่สำคัญ**

อนึ่ง ในปัจจุบันยังไม่ได้มีการให้คำอธิบายหรือคำวินิจฉัยอย่างเป็นทางการจากคณะกรรมการ แต่ถ้ายึดเทียบเคียงกับการปรับใช้ของ GDPR ข้อ 9(2)(g) ซึ่งให้อำนาจประเทศสมาชิกในการกำหนดว่าอะไรคือประโยชน์สาธารณะที่สำคัญ โดยการกำหนดประโยชน์สาธารณะที่สำคัญดังกล่าวจะต้องได้สัดส่วนและเคารพซึ่งสิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง

- การปฏิบัติหน้าที่ของหน่วยงานของรัฐ
- การดำเนินการเพื่อสร้างความเท่าเทียม
- การดำเนินการเพื่อสร้างความหลากหลายด้านชาติพันธุ์
- การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย
- การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต (ซึ่งหมายรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต)

⁷² มาตรา 26 (5) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- การป้องกันการฉ้อฉล
- การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน
- การให้ความช่วยเหลือบุคคลผู้พิการหรือต้องได้รับความช่วยเหลือทางการแพทย์
- การช่วยเหลือเด็กหรือผู้ที่ตกอยู่ในภาวะเสี่ยง
- บำนาญ
- พรรคการเมือง
- การเผยแพร่คำพิพากษา

(3) บริษัทได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

สำหรับการดำเนินการของบริษัท โดยเฉพาะในส่วนของการรับประกันภัยส่วนบุคคลที่มีผลิตภัณฑ์หลายประเภท เช่น ประกันภัยสุขภาพ ประกันภัยการเดินทางไปต่างประเทศ ฯลฯ มีลักษณะการดำเนินธุรกิจที่ต้องอาศัยการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวจำนวนมาก เช่น ข้อมูลสุขภาพ ประวัติการรักษาพยาบาล ข้อมูลการตอบคำถามสุขภาพ ไม่เหมือนกับการดำเนินธุรกิจอื่น ๆ ซึ่งไม่มีการใช้ข้อมูลสุขภาพเป็นการทั่วไป ซึ่งการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าวนี้ใช้เพื่อการพิจารณารับประกันภัย พิจารณาจ่ายค่าสินไหมทดแทน ตลอดจนป้องกันการฉ้อโกงประกันภัย ทั้งนี้ เมื่อพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลแล้ว อาจพิจารณา และตีความได้ว่าหากข้อมูลส่วนบุคคลใด (โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่มีความอ่อนไหว) จำเป็นต่อการประมวลผลเพื่อการเข้าทำสัญญาประกันภัย และการชดเชยค่าสินไหมทดแทน บริษัทควรที่จะดำเนินการตามแนวทางดังต่อไปนี้ได้

1. บริษัทไม่ต้องขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล (ทั่วไป) โดยอ้างอิงข้อยกเว้นตามมาตรา 24 (3) การเข้าทำสัญญาประกันภัยและการปฏิบัติตามสัญญาประกันภัย

2. บริษัทไม่ต้องขอความยินยอมโดยชัดแจ้งสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal data) โดยพิจารณาถึงฐานการประมวลผลข้อมูลส่วนบุคคลมาตรา 24 (3) การปฏิบัติตามสัญญาประกันภัย และอ้างอิงข้อยกเว้นของการขอความยินยอมเกี่ยวกับการก่อตั้งสิทธิเรียกร้องตามกฎหมายตามมาตรา 26 (4) หรือประโยชน์สาธารณะที่สำคัญตามมาตรา 26 (5) (จ)

5.3 การเปลี่ยนวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

โดยหลัก บริษัทจะต้องประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวเท่านั้น อย่างไรก็ตาม บริษัทสามารถประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งกับเจ้าของข้อมูลส่วนบุคคลนั้นได้ หาก บริษัทดำเนินการ ดังนี้⁷³

(1) แจ้งเจ้าของข้อมูลส่วนบุคคลถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลใหม่ และ

(2) ได้รับความยินยอมสำหรับวัตถุประสงค์ใหม่นั้นจากเจ้าของข้อมูลส่วนบุคคล ก่อน ทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ดังกล่าว

เว้นแต่ในกรณีที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นให้อำนาจบริษัทในการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่นอกเหนือจากที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคลอยู่แล้ว บริษัทดำเนินการตามที่กฎหมายกำหนดได้ทันที โดยไม่จำเป็นต้องดำเนินการตามข้อ 1 และ 2 ข้างต้นก็ได้

ข้อพิจารณาเบื้องต้น⁷⁴

- บริษัทได้ตั้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลไว้อย่างชัดเจนแล้ว
- บริษัทได้จัดบันทึกวัตถุประสงค์ดังกล่าวแล้ว
- บริษัททรมารายละเอียดของวัตถุประสงค์ข้างต้น ไว้ในข้อมูลเกี่ยวกับความเห็นส่วนตัวให้ไว้กับเจ้าของข้อมูลส่วนบุคคลแล้ว
- บริษัทตรวจสอบการประมวลผลข้อมูลอย่างสม่ำเสมอ และเมื่อจำเป็นบริษัทปรับปรุงรายการจัดบันทึกและข้อมูลเกี่ยวกับความเห็นส่วนตัวให้แก่เจ้าของข้อมูลส่วนบุคคล
- หากต้องการจะประมวลผลข้อมูลส่วนบุคคลเพื่อกิจกรรมใหม่ บริษัทต้องหาวัตถุประสงค์ของกิจกรรมดังกล่าวก่อน และตรวจสอบว่าวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบไปแล้วครอบคลุมถึงกิจกรรมใหม่ที่จะดำเนินการหรือไม่

⁷³ มาตรา 21 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

⁷⁴ เทียบเคียงกับ Information Commissioner's Office, UK (ICO), 'Principle (b): Purpose limitation', ICO < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/> > accessed 15 April 2020

- หากกิจกรรมใหม่ครอบคลุมอยู่ในวัตถุประสงค์ที่แจ้งเจ้าของข้อมูลส่วนบุคคลแล้ว บริษัทสามารถดำเนินการดังกล่าวได้ทันที ไม่จำเป็นต้องดำเนินการใด ๆ
- หากกิจกรรมใหม่นั้นไม่รวมอยู่ในวัตถุประสงค์ที่เคยแจ้งเจ้าของข้อมูลส่วนบุคคลแล้ว และวัตถุประสงค์ที่จะใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ใหม่ ไม่ได้เป็นไปตามหน้าที่หรือภารกิจที่กำหนดโดยกฎหมาย บริษัทจะต้องแจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะเจาะจงสำหรับวัตถุประสงค์ใหม่นั้น

ตัวอย่าง

เดิมบริษัทเก็บรวบรวมข้อมูลเชื้อชาติหรือเผ่าพันธุ์ของผู้เอาประกันภัยเพื่อพิจารณารับประกันการเดินทาง ต่อมาบริษัทต้องการเปิดเผยข้อมูลดังกล่าวของผู้เอาประกันภัยแก่บริษัท เอ ซึ่งเป็นผู้ให้บริการการท่องเที่ยว โดยบริษัท เอ ต้องการเสนอส่วนลดการจองที่พักให้แก่ผู้เอาประกันภัยเดินทางที่เป็นคนเอเชียตะวันออกเฉียงใต้ เช่นนี้ วัตถุประสงค์เดิมที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อประเมินความเสี่ยงและรับประกันภัยเดินทางนั้น แตกต่างกับวัตถุประสงค์ใหม่ของบริษัทที่ต้องการเปิดเผยข้อมูลดังกล่าวแก่บริษัท เอ เพื่อให้มีการเสนอส่วนลดการจองที่พักแก่ผู้เอาประกันภัยเดินทาง เช่นนี้ บริษัทต้องดำเนินการแจ้ง และขอความยินยอมโดยชัดแจ้ง (เพราะกรณีนี้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว) จากเจ้าของข้อมูลส่วนบุคคลก่อนดำเนินการประมวลผลข้อมูลส่วนบุคคลดังกล่าวภายใต้วัตถุประสงค์ใหม่

5.4 แนวทางการกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

เมื่อพิจารณา พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 22 แล้ว จะสังเกตได้ว่า กฎหมายไม่ได้มีการกำหนดระยะเวลาที่ชัดเจนสำหรับการเก็บรักษาข้อมูลส่วนบุคคลในแต่ละประเภท เพียงแต่กำหนดว่า “การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล” ประกอบกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 23 ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดเกี่ยวกับ “ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” แล้ว ดังนั้น พอจะได้ข้อสรุปว่า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล อนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรักษาข้อมูลส่วนบุคคลได้นานเท่าที่จำเป็นภายใต้วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลแต่ละเรื่องเท่านั้น และจะต้องมีการกำหนดและแจ้งกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวนี้อย่างชัดแจ้ง และผู้ควบคุมข้อมูลส่วนบุคคลจะไม่สามารถเก็บรักษาข้อมูลส่วนบุคคลไว้ได้ตลอดไป

ทั้งนี้ ในเรื่องกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลนั้น ขึ้นอยู่กับความจำเป็นในการเก็บรักษาเพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้น ๆ

ข้อเสนอแนะ

บริษัทผู้ซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล ควรดำเนินการดังต่อไปนี้ เพื่อให้สามารถกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล โดยเป็นไปตามหลักเกณฑ์ของ พ.ร.บ. คัมครองข้อมูลส่วนบุคคล

- (1) จัดทำรายการกิจกรรม และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลทั้งหมดของบริษัท โดยแบ่งแยกตามประเภทของเจ้าของข้อมูลส่วนบุคคล เช่น ลูกค้า พนักงาน ผู้สมัครงาน คู่ค้า ผู้ให้บริการ หรือผู้ขายสินค้า (Vendors/Suppliers) เป็นต้น
- (2) กำหนดระยะเวลาที่จำเป็นต้องประมวลผลข้อมูลส่วนบุคคลสำหรับแต่ละกิจกรรม หรือวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลไว้ โดยอาจมีการระบุหลักการที่ใช้อ้างอิงในการกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล เช่น ระยะเวลาตามที่กฎหมายกำหนด ระยะเวลาตามสัญญา หรือระบุเหตุผลของการกำหนดระยะเวลานั้น ๆ ทั้งนี้ เพื่อให้บริษัทมีหลักฐานว่าบริษัทได้ดำเนินการประเมินความจำเป็นในการเก็บรวบรวมข้อมูลส่วนบุคคลเหล่านั้นแล้ว โดยเอกสารที่บริษัทพิจารณาระบุระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลนี้ (Data Retention Policy/ Data Retention Schedules) ควรเก็บเอาไว้ในกรณีที่มีการตรวจสอบโดยคณะกรรมการ
- (3) ระบุระยะเวลาที่กำหนดไว้ในนโยบายคุ้มครองความเป็นส่วนตัวของบริษัทที่แจ้งต่อเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล⁷⁵
- (4) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาที่ระบุไว้⁷⁶ และ
- (5) จัดทำบันทึกเกี่ยวกับกำหนดระยะเวลาในข้อ (1) เตรียมไว้เพื่อให้เจ้าของข้อมูลส่วนบุคคลหรือสำนักงานสามารถตรวจสอบได้ เมื่อร้องขอ⁷⁷

ตัวอย่างการพิจารณาความจำเป็นของระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

- บริษัทควรเก็บข้อมูลส่วนบุคคลของลูกค้าไว้เป็นเวลาอย่างน้อย 10 ปี นับแต่วันที่สิ้นสุดความสัมพันธ์กับลูกค้า เนื่องจากการปฏิบัติตามกฎหมายฟอกเงิน⁷⁸

⁷⁵ มาตรา 23 (3) พ.ร.บ. คัมครองข้อมูลส่วนบุคคล

⁷⁶ มาตรา 37 (3) พ.ร.บ. คัมครองข้อมูลส่วนบุคคล

⁷⁷ มาตรา 39 (4) พ.ร.บ. คัมครองข้อมูลส่วนบุคคล

⁷⁸ มาตรา 60 พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน และมาตรา 95 (2) ป.อ.

- บริษัทสามารถเก็บข้อมูลส่วนบุคคลของนายหน้าประกันวินาศภัยไว้ได้ 10 ปี นับแต่วันสิ้นสุดสัญญา สำหรับกรณีที่บริษัทจะฟ้องเรียกให้นายหน้าส่งมอบเบี้ยประกันภัยที่รับมา แต่ไม่ได้ส่งให้บริษัท เนื่องจากเป็นการอ้างอิงตามอายุความในการฟ้องคดีแพ่ง⁷⁹
- เมื่อบริษัทได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลให้หยุดส่งข้อความโฆษณาหรือโทรศัพท์ไปหาเพื่อเสนอขายผลิตภัณฑ์ภายใต้การทำการตลาดโดยตรงของบริษัท เช่นนี้ บริษัทมีความจำเป็นที่จะต้องเก็บรักษาข้อมูลส่วนบุคคลบางส่วนไว้เพื่อป้องกันไม่ให้เกิดการติดต่อลูกค้าของบริษัท ลูกค้าคนดังกล่าวอีก ในการทำการตลาดโดยตรงครั้งต่อไป
- บริษัทอาจเก็บข้อมูลส่วนบุคคลของพนักงานบริษัท ซึ่งได้ออกจากงานไปแล้วได้ด้วยเหตุผลที่ว่า จำเป็นจะต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวเพื่อปฏิบัติตามภาระผูกพันที่มีต่อพนักงานคนนั้น ๆ (เช่น การออกหนังสือรับรอง หรือการปฏิบัติตามข้อตกลงเกี่ยวกับผลประโยชน์หลังเกษียณอายุงาน)

ข้อสังเกต

- กรณีที่มีกฎหมายหรือข้อบังคับใด กำหนดระยะเวลาให้บริษัทจัดเก็บหรือบันทึกข้อมูลส่วนบุคคลเอาไว้ เช่นนี้ ถือได้ว่ามีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวแล้ว
- บริษัทควรจะเก็บรักษาข้อมูลส่วนบุคคลไว้เท่าที่จำเป็น สำหรับปฏิบัติตามที่กฎหมายกำหนดเท่านั้น เช่น ข้อมูลส่วนบุคคลต่าง ๆ ที่บริษัทจำเป็นจะต้องเก็บรวบรวม ในกรณีการปฏิบัติตาม พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน ส่วนข้อมูลส่วนบุคคลบางอย่างที่ไม่จำเป็น เช่น ข้อมูลบุคคลที่ติดต่อในกรณีฉุกเฉิน หรือข้อมูลบุคคลผู้รับประโยชน์ หากไม่จำเป็นต้องเก็บรักษาไว้เพื่อการป้องกันและปราบปรามการฟอกเงินนี้ บริษัทไม่ควรเก็บรักษาไว้ (เว้นแต่มีความจำเป็นอื่น)
- สำหรับกรณีที่บริษัทมีความสัมพันธ์ หรือมีสัญญากับเจ้าของข้อมูลส่วนบุคคล บริษัทอาจกำหนดระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลหลังจากสิ้นสุดความสัมพันธ์ระหว่างกันได้ กล่าวคือ เก็บรักษาข้อมูลส่วนบุคคลไว้ตลอดระยะเวลาที่มีความสัมพันธ์กัน และเมื่อสิ้นสุดความสัมพันธ์ บริษัทอาจกำหนดระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวไว้ ทั้งนี้ บริษัทต้องคำนึงถึงความจำเป็นด้วย
- หากความจำเป็นของบริษัท คือ การเก็บข้อมูลส่วนบุคคลไว้ “เผื่อว่าจำเป็นจะต้องใช้” หรือมีความเป็นไปได้เพียงเล็กน้อยที่จะต้องใช้เช่นนี้ บริษัทจะอ้างไม่ได้ว่ามีความจำเป็นในการเก็บรักษาข้อมูล

⁷⁹ มาตรา 193/30 ป.พ.พ.

ส่วนบุคคลดังกล่าว ทั้งนี้ บริษัทจะต้องไม่ลืมว่า วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่บริษัทอ้างอิงจะต้องชอบด้วยกฎหมายเสมอ

- กระบวนการพิจารณากำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Policy หรือ Data Retention Schedules) สามารถบันทึกไว้เป็นส่วนหนึ่งของบันทึกตามรายการของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 ได้
- บริษัทสามารถลบหรือทำลายข้อมูลส่วนบุคคลนั้นก่อนระยะเวลาที่กำหนดไว้สำหรับการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวได้ แม้ว่าบริษัทจะได้กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเอาไว้แล้ว โดยที่บริษัทมีเหตุจะต้องลบหรือทำลาย (เช่น เจ้าของข้อมูลส่วนบุคคลร้องขอ) ทั้งนี้ บริษัทควรจะต้องจดบันทึกเหตุในการลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวไว้ด้วย

5.5 แนวทางการส่งหรือโอนข้อมูลส่วนบุคคลในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันในประเทศ

ในเรื่องการส่ง หรือโอนข้อมูลส่วนบุคคลในกลุ่มเครือกิจการ หรือเครือธุรกิจเดียวกันในประเทศนั้น ทั้ง GDPR และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ล้วนไม่ได้มีการกำหนดเงื่อนไข ข้อกำหนด หรือวิธีการดำเนินการในเรื่องดังกล่าวนี้เป็นการเฉพาะเหมือนกับเรื่องการโอนข้อมูลส่วนบุคคลไปยังกลุ่มเครือกิจการ หรือเครือธุรกิจที่ตั้งอยู่ในต่างประเทศ ดังนั้น เงื่อนไข วิธีการ และขั้นตอนในการดำเนินการเกี่ยวกับส่งหรือโอนข้อมูลส่วนบุคคลในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันในประเทศนั้น จึงต้องพิจารณา และดำเนินการตามหลักเกณฑ์ทั่วไปที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งโดยหลักการแล้ว การดำเนินการส่ง หรือโอนข้อมูลส่วนบุคคลให้บริษัทในเครือนั้น เป็นการเปิดเผยข้อมูลให้บุคคลอื่น หรือองค์กรอื่นทราบ ดังนั้น การดำเนินการดังกล่าวนี้ จึงต้องคำนึงถึงในทุกครั้งที่เกี่ยวเนื่องกับการเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องพิจารณาเมื่อจะมีการส่งหรือโอนข้อมูลส่วนบุคคลในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันในประเทศ มีดังนี้

- กำหนดความสัมพันธ์ระหว่างบริษัท กับ บริษัทในกลุ่มเครือกิจการ หรือเครือธุรกิจเดียวกันว่าตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แต่ละฝ่ายมีสถานะที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอย่างไร กล่าวคือ การโอนข้อมูลส่วนบุคคลดังกล่าว ฝ่ายใดมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล หรือทั้งสองฝ่าย (หรือหลายฝ่าย) ต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งการจะกำหนดสถานะของแต่ละบริษัทได้นั้น บริษัทจะต้องพิจารณาลักษณะของการส่ง หรือโอนข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง วัตถุประสงค์ของการโอนข้อมูลส่วนบุคคล

- **รายละเอียดเกี่ยวกับการส่ง หรือโอนข้อมูลส่วนบุคคล** กล่าวคือ บริษัทต้องพิจารณาว่าข้อมูลส่วนบุคคลใดบ้างที่จะถูกส่ง หรือโอน เจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องคือใคร วัตถุประสงค์ของการส่ง หรือโอนข้อมูลส่วนบุคคลนั้นเป็นอย่างไร ซึ่งรายละเอียดดังกล่าวนี้บริษัทจะต้องบันทึกลงในรายละเอียดการประมวลผลข้อมูลส่วนบุคคล หรือ Record of Processing Activities (ROPA) รวมถึงต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบตามมาตรา 23 ด้วยเช่นกัน
- **วิธีการส่ง หรือโอนข้อมูลส่วนบุคคล** กล่าวคือ ตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวที่กำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล บริษัทมีหน้าที่ต้องจัดให้มีมาตรการการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และหากมีการเปิดเผย หรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล บริษัทจะต้องดำเนินการเพื่อป้องกันมิให้ผู้รับใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ดังนั้นในการส่ง หรือโอนข้อมูลส่วนบุคคลระหว่างบริษัทในกลุ่มเครือกิจการที่อยู่ในประเทศไทย บริษัทมีหน้าที่ต้องดำเนินการในเรื่องดังกล่าวนี้ด้วย
- **ในกรณีที่ผู้รับข้อมูลส่วนบุคคลเป็นผู้ประมวลผลข้อมูลส่วนบุคคล** – บริษัทจะต้องดำเนินการจัดให้มีการเข้าทำสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ด้วยเช่นกัน

5.6 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น⁸⁰

5.6.1 หลักการและข้อยกเว้นในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

หลัก ห้ามไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

ข้อยกเว้น

1) กรณีที่ฐานในการประมวลผลคือฐานความยินยอม

หากผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังนี้

⁸⁰ มาตรา 25 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

(ก) แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น รวมถึงรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 23 โดยไม่ชักช้า แต่ต้องไม่เกิน 30 วัน นับแต่วันที่เก็บรวบรวม

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งรายละเอียดข้างต้นในกรณีดังต่อไปนี้

- เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์หรือรายละเอียดนั้นอยู่แล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าว ไม่สามารถทำได้ หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

ข้อยกเว้นเรื่องระยะเวลาในการแจ้งรายละเอียด

ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 21 ได้ในกรณีต่อไปนี้

- กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อกครั้งแรก
- กรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

(ข) ขอและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2) กรณีฐานในการประมวลผลไม่ใช้ฐานความยินยอม

ในกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยฐานการประมวลผลไม่ใช่ฐานความยินยอมตามมาตรา 24 หรือมาตรา 26 นั้น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลอนุญาตให้ทำได้โดยเป็นข้อยกเว้น และผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องขอความยินยอม และไม่ต้องแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นรวมถึงรายละเอียดตามมาตรา 23 อีก

ตัวอย่างการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยไม่ได้อ้างอิงฐานความยินยอม

กรณีที่น่าายหนึ่ง ระบุชื่อ นางสาว เป็นผู้รับประโยชน์ในสัญญาประกันภัยอุบัติเหตุการเดินทางที่ทำกับบริษัท ซี เช่นนี้ บริษัท ซี เก็บรวบรวมข้อมูลส่วนบุคคลของนางสาวมาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลเอง แต่เนื่องจากการประมวลผลข้อมูลส่วนบุคคลของนางสาวนั้นเป็นไปเพื่อประโยชน์ในการดำเนินการเกี่ยวกับการจ่ายค่าสินไหมทดแทนตามกรมธรรม์ประกันภัยที่นายหนึ่ง เข้าทำกับบริษัท ซี การประมวลผลข้อมูลส่วนบุคคลของนางสาวจึงอยู่บนฐานประโยชน์อันชอบธรรม (ไม่ใช่ฐานสัญญาเนื่องจากนางสาวไม่ใช่คู่สัญญากับบริษัท ซี) ดังนั้น ในกรณีนี้บริษัท ซี ไม่ต้องดำเนินการขอความยินยอมและแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลในนางสาว

ข้อสังเกต

ตาม GDPR⁸¹ การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ ไม่ว่าฐานในการประมวลผลจะอยู่บนฐานความยินยอม หรือไม่ได้อยู่บนฐานความยินยอม แต่เนื่องจากบทบัญญัติมาตรา 25 เรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลนั้นเขียนไว้แตกต่างจากบทบัญญัติของ GDPR หลักการจึงต่างกันไปตามที่บัญญัติ

5.6.2 แนวทางเพิ่มเติมในการเก็บข้อมูลจากแหล่งอื่น ที่มีลักษณะเป็นตัวกลางประกันภัยหรือคู่ค้า
เพื่อการทำคำเสนอผลิตภัณฑ์เป็นการเฉพาะ (Quotation/ Proposal) หรือเพื่อการออกกรมธรรม์ประกันภัย

กรณีการเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงหากเป็นไปเพื่อการจำเป็นในการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา (ตามมาตรา 25 (2) ประกอบมาตรา 24 (3)) หรือเป็นข้อมูลส่วนบุคคลที่ไม่มีลักษณะเป็นข้อมูลอ่อนไหว (ไม่ใช่ Sensitive Personal Data ตามมาตรา 26)

บริษัทไม่มีหน้าที่ต้อง (ก) ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ (ข) ไม่ต้องแจ้งรายละเอียดที่เกี่ยวข้อง (โดยใช้ Privacy Policy/Notice)

⁸¹ Article 14 of the GDPR

ดังนั้น หากเป็นการเก็บข้อมูลส่วนบุคคลของผู้ขอเอาประกันภัย ซึ่งได้ทำคำขอเพื่อขอทำประกันผ่านนายหน้าประกันวินาศภัย หรือคู่ค้าอื่นโดยที่ผู้ขอเอาประกันภัยทราบและให้ข้อมูลดังกล่าวเพื่อการขอเข้าทำประกันภัย หรือขอคำแนะนำราคาและความคุ้มครองเป็นการเฉพาะให้แก่ผู้ขอเอาประกันภัย บริษัทไม่มีหน้าที่ตามมาตรา 25 ในการขอความยินยอมและแจ้งข้อมูลรายละเอียดที่เกี่ยวข้อง (โดยใช้ Privacy Policy/Notice) เพื่อการปฏิบัติตามกฎหมายนี้

ทั้งนี้ หากเป็นกรณีการดำเนินการดังกล่าวโดยตัวแทนประกันวินาศภัยของบริษัท เนื่องจากตัวแทนประกันวินาศภัยทำการในนามของบริษัทจึงไม่ถือได้ว่าเป็นการเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นตามข้อกำหนดของมาตรา 25 นี้ แต่เป็นการที่ตัวแทนประกันภัยดำเนินการในฐานะของผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัท

5.6.3 แนวทางเพิ่มเติมในการเก็บข้อมูลจากแหล่งอื่น เพื่อการนำข้อมูล (Lead) มาเสนอขายผลิตภัณฑ์โดยที่เจ้าของข้อมูลส่วนบุคคลยังไม่ได้แสดงเจตนาขอเข้าทำประกันภัยหรือคำแนะนำเฉพาะ

กรณีการเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงหากเป็นไปเพื่อ

1. การนำ/ซื้อ Lead ข้อมูลมาเพื่อวัตถุประสงค์การเสนอขายผลิตภัณฑ์ หรือดำเนินกิจกรรมทางการตลาด

2. Lead ประกอบด้วยข้อมูลส่วนบุคคลทั่วไป (ไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหว) หมายถึง ชื่อ-นามสกุล และหมายเลขโทรศัพท์

3. แหล่งข้อมูลอื่น เช่น คู่ค้าของบริษัทมีหน้าที่ขอความยินยอมในการเปิดเผยข้อมูลดังกล่าวตั้งแต่ต้นทาง โดยบริษัท อาจตกลงกับคู่ค้าของบริษัทให้ดำเนินการดังต่อไปนี้

3.1 แนวทางการขอความยินยอมจากต้นทางโดยการระบุชื่อบริษัทประกันวินาศภัยเป็นการเฉพาะ

ในกรณีที่คู่ค้าตกลงกับบริษัทว่าคู่ค้าจะขอความยินยอมจากลูกค้า หรือผู้มุ่งหวังมาให้บริษัท โดยการระบุชื่อบริษัทขอความยินยอม บริษัทควรจัดให้คู่ค้าของบริษัท ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลพร้อมแจ้งรายละเอียดเบื้องต้นของบริษัท เช่น ชื่อบริษัท และวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลที่บริษัทจะนำข้อมูลดังกล่าวมาใช้ในการเสนอขายผลิตภัณฑ์ประกันวินาศภัย ซึ่งในกรณีดังกล่าวนี้เนื่องจากลูกค้ารับรู้รับทราบแล้วว่าบริษัท (ตามที่ระบุชื่อ) จะทำการติดต่อเพื่อการเสนอขายผลิตภัณฑ์ประกันวินาศภัย เมื่อบริษัททำการเสนอขายผลิตภัณฑ์เป็นครั้งแรก บริษัทจึงไม่ต้องขอความยินยอมซ้ำอีกครั้งหนึ่งและสามารถใช้และประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ต่อไปตามขอบเขตที่คู่ค้าได้ขอความยินยอมให้แล้วจากต้นทางขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล

3.2 แนวทางการขอความยินยอมจากต้นทางโดยไม่ระบุชื่อบริษัทประกันวินาศภัยเป็นการเฉพาะ

ในกรณีที่คู่ค้าไม่สามารถระบุชื่อบริษัท เป็นการเฉพาะขณะที่ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ บริษัทอาจตกลงกับคู่ค้าของบริษัทให้คู่ค้าดังกล่าวขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยการระบุว่าเป็นความยินยอมให้ “บริษัทประกันวินาศภัย” หรือ “ภาคธุรกิจประกันวินาศภัย/ธุรกิจประกันภัย” ใช้ในการติดต่อเสนอผลิตภัณฑ์ประกันวินาศภัยได้ซึ่งในกรณีนี้เมื่อบริษัทได้รับข้อมูลส่วนบุคคลมาแล้ว บริษัทจะดำเนินการเสนอขายประกันวินาศภัยของบริษัท ในขั้นตอนที่ติดต่อเจ้าของข้อมูลส่วนบุคคลในครั้งแรกนั้น บริษัทจะต้องดำเนินการดังต่อไปนี้

(1) เมื่อบริษัทติดต่อกับเจ้าของข้อมูลส่วนบุคคลเพื่อเสนอขาย บริษัทควรอธิบายถึงขั้นตอนการได้ข้อมูลดังกล่าว และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของบริษัท ให้แก่เจ้าของข้อมูลส่วนบุคคลทราบอย่างชัดเจน เช่น แจ้งว่าบริษัทได้รับข้อมูลส่วนบุคคลมาจากแหล่งใด และทำการติดต่อเจ้าของข้อมูลส่วนบุคคลเพื่อการเสนอขายผลิตภัณฑ์ หากเจ้าของข้อมูลส่วนบุคคลคัดค้านการเสนอขายผลิตภัณฑ์ดังกล่าว บริษัทควรหยุดการสนทนาและการเสนอขาย เพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องกับการเสนอขายผลิตภัณฑ์ประกันวินาศภัย

ในกรณีนี้ บริษัทจำเป็นต้องเชื่อถือคำรับรองและอาศัยคู่ค้าในการขอความยินยอมจากลูกค้าให้กับบริษัท ดังนั้น บริษัทควรกำหนดมาตรการในการประเมินและบริหารความเสี่ยงตามความเหมาะสมของบริษัท เช่น การทำคำรับรอง การเข้าทำสัญญากำหนดสิทธิหน้าที่ของคู่สัญญา วิธีการตรวจสอบอื่นใดตามที่ตกลงกัน หรือการบริหารจัดการเรื่องร้องเรียน

5.6.4 กรณีที่ได้รับ Lead มาก่อนหน้าวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับทั้งฉบับ

เนื่องด้วยมาตรา 95 อนุญาตให้ผู้ควบคุมข้อมูลส่วนบุคคลยังสามารถเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลที่มีอยู่ก่อนได้ ภายใต้วัตถุประสงค์เดิม ดังนั้น หากคู่ค้าของบริษัท ได้ขอความยินยอมแล้วในลักษณะดังกล่าว และส่ง Lead ให้กับบริษัท แล้ว บริษัทย่อมสามารถใช้ lead นั้นในการทำการตลาด หรือเสนอขายได้ โดยคู่ค้าหรือบริษัทไม่จำเป็นต้องขอความยินยอมอีกครั้งหนึ่ง ทั้งนี้ บริษัทยังคงต้องมีหน้าที่อื่นในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (ตามมาตรา 95 และมาตราอื่นที่เกี่ยวข้อง) แม้ว่าไม่ต้องขอความยินยอมซ้ำ

5.6.5 แนวทางเพิ่มเติมเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นเพื่อการทำประกันภัยกลุ่ม

ในการเข้าทำประกันภัยกลุ่มนั้น บริษัทควรดำเนินการตามแนวทางดังต่อไปนี้

1. บริษัทกำหนดเงื่อนไขในใบคำขอเอาประกันภัย กรมธรรม์ประกันภัย หรือเอกสารอื่นใด ให้ผู้เอาประกันภัยซึ่งเป็นนายจ้าง ให้คำรับรอง (Representation and Warranty) ว่าได้แจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของบริษัทให้กับลูกจ้างของบริษัทลูกค้าแล้ว
2. บริษัทไม่ต้องขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล โดยอ้างอิงข้อยกเว้นตามมาตรา 24 (3) การเข้าทำสัญญาประกันภัยและการปฏิบัติตามสัญญาประกันภัย กรณีที่มีการให้ข้อมูลส่วนบุคคลของผู้รับผลประโยชน์ให้อ้างอิงข้อยกเว้นตามมาตรา 24 (5)
3. บริษัทไม่ต้องขอความยินยอมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลที่อ่อนไหว โดยพิจารณาถึงฐานการประมวลผลข้อมูลส่วนบุคคลมาตรา 24 (3) การปฏิบัติตามสัญญาประกันภัย และอ้างอิงข้อยกเว้นของการขอความยินยอมที่เกี่ยวกับการก่อตั้งสิทธิเรียกร้องตามกฎหมายตามมาตรา 26 (4) หรือประโยชน์สาธารณะที่สำคัญตามมาตรา 26 (5) (จ)

5.7 แนวทางการบันทึกการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 ผู้ควบคุมข้อมูลส่วนบุคคล และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (Local Representative) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่ต่างประเทศ จะต้องจัดทำรายการบันทึกอย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคล และสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล เช่น ชื่อและรายละเอียดการติดต่อของบริษัท ของผู้แทนบริษัท หรือของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท
4. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
6. การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ในกรณีที่มีการอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่นนอกจากฐานความยินยอม

7. การปฏิเสธคำขอหรือการคัดค้าน พร้อมด้วยเหตุผลในการปฏิเสธ เช่น

- 7.1 กรณีเจ้าของข้อมูลส่วนบุคคลขอเข้าถึงและรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของบริษัท หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม
- 7.2 กรณีเจ้าของข้อมูลส่วนบุคคลขอให้ส่งหรือโอนข้อมูลส่วนบุคคลไปให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่น แต่การส่งหรือโอนข้อมูลดังกล่าวกระทำไม่ได้เพราะผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ตามกฎหมาย
- 7.3 กรณีเจ้าของข้อมูลส่วนบุคคลขอให้ส่งหรือโอนข้อมูลส่วนบุคคลไปให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่น แต่การส่งหรือโอนข้อมูลดังกล่าวจะทำให้ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น
- 7.4 กรณีเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในการประมวลผลข้อมูลส่วนบุคคลที่อ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม แต่บริษัทสามารถแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
- 7.5 กรณีเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในการประมวลผลข้อมูลส่วนบุคคลที่อ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม แต่การประมวลผลข้อมูลดังกล่าว เป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- 7.6 กรณีเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในการประมวลผลข้อมูลส่วนบุคคลเพื่่วัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ซึ่งเป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
- 7.7 กรณีเจ้าของข้อมูลส่วนบุคคลร้องขอให้บริษัทดำเนินการทำให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของบริษัท ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (1)

ตัวอย่างแบบการบันทึกการประมวลผลข้อมูลส่วนบุคคล

โปรดดูตัวอย่างการบันทึกการประมวลผลข้อมูลส่วนบุคคลในบทที่ 11

5.8 แนวทางการแลกเปลี่ยนข้อมูลส่วนบุคคลที่กระทำความผิดอาญาเกี่ยวกับการประกันวินาศภัย

ปัจจุบัน พ.ร.บ. ประกันวินาศภัย ได้กำหนดความผิดและโทษอาญาไว้โดยเฉพาะสำหรับการกระทำความผิดเกี่ยวกับประกันวินาศภัยในเรื่องของการฉ้อฉล ซึ่งแม้จะเป็นประโยชน์ต่อการดำเนินธุรกิจประกันวินาศภัยในด้านการป้องกันการกระทำความผิด แต่ในทางปฏิบัติก็ทำให้เกิดคำถามเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการแลกเปลี่ยนข้อมูลส่วนบุคคลดังกล่าวเพื่อเตือนภัยและป้องกันการกระทำความผิดซ้ำซึ่งเป็นแนวทางปฏิบัติปกติ ในเรื่องของการแลกเปลี่ยนข้อมูลประวัติอาชญากรรมอันเกี่ยวกับความผิดข้างต้น เช่น ความผิดทางอาญาที่เกี่ยวข้องกับตัวแทนหรือนายหน้า ความผิดอาญาเกี่ยวกับการฉ้อฉลการประกันภัยบริษัท จะต้องดำเนินการให้เป็นไปตามเงื่อนไขที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด ดังนี้

- บริษัทจะต้องกระทำการแลกเปลี่ยนข้อมูลประวัติอาชญากรรม โดยอยู่ภายใต้การควบคุมของกองทะเบียนประวัติอาชญากรรม สำนักงานตำรวจแห่งชาติ ซึ่งมีอำนาจหน้าที่จัดทำและดูแลประวัติอาชญากรรมตามกฎหมาย หรือ
- บริษัทจะต้องกระทำการแลกเปลี่ยนข้อมูลประวัติอาชญากรรม โดยมีมาตรการคุ้มครองข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด (ซึ่งปัจจุบัน คณะกรรมการยังไม่ได้ประกาศกำหนด)

ข้อสังเกต

- เมื่อมีการใช้ หรือเปิดเผยข้อมูลประวัติอาชญากรรมข้างต้น เช่น การแลกเปลี่ยนข้อมูลภายในสมาคมแล้ว บริษัทที่กระทำการใช้ หรือเปิดเผยข้อมูลประวัติอาชญากรรมนั้น จะต้องทำการบันทึกลงในรายการ ตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย
- ในทางปฏิบัติ เมื่อการตั้งข้อกล่าวหาในชั้นสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจ ก็จะมีการบันทึกประวัติอาชญากรรมไว้ ในฐานะข้อมูลของกองทะเบียนประวัติอาชญากรรม สำนักงานตำรวจแห่งชาติแล้ว

บทที่ 6 การโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ

แนวทางปฏิบัติเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ

6.1 หลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล⁸² กำหนดให้ ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลต้องการที่จะส่งหรือโอนข้อมูลส่วนบุคคลออกไปนอกประเทศไทย (ไม่ว่าจะเป็นต่างประเทศ หรือองค์กรระหว่างประเทศ) ปลายทางต่างประเทศที่จะรับข้อมูลส่วนบุคคลดังกล่าวต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ มาตรฐานการคุ้มครองดังกล่าวจะต้องเป็นไปตามคณะกรรมการการประกาศกำหนด

นอกจากนี้ หากบริษัทมีข้อสงสัยเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของปลายทางต่างประเทศที่จะรับข้อมูลส่วนบุคคลข้างต้น บริษัทอาจเสนอให้คณะกรรมการเป็นผู้วินิจฉัยได้ ทั้งนี้ บริษัทอาจขอให้มีการทบทวนคำวินิจฉัยนั้นใหม่ได้ เมื่อมีหลักฐานว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของปลายทางต่างประเทศได้มีการพัฒนาจนเพียงพอแล้ว

ข้อสังเกต

หากข้อมูลส่วนบุคคลถูกเก็บรวบรวมเป็นครั้งแรกโดยบุคคลในต่างประเทศ การเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว ไม่ถือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ

6.2 ข้อยกเว้นของเงื่อนไขในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ข้อยกเว้นทั่วไป

แม้ว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของปลายทางต่างประเทศที่จะรับข้อมูลส่วนบุคคลจะไม่เพียงพอ ตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด บริษัทก็ยังสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศดังกล่าวได้ หากเป็นกรณีการส่งหรือโอนข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

1. เป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยเป็นการปฏิบัติตามกฎหมาย
2. เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม เมื่อได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของปลายทางต่างประเทศ

⁸² มาตรา 28 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6. เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

6.3 ข้อยกเว้นสำหรับการโอนข้อมูลส่วนบุคคลไปยังบริษัทในเครือ หรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน

หากบริษัทมี “นโยบายในการคุ้มครองข้อมูลส่วนบุคคลภายในเครือกิจการ” (Binding Corporate Rules: BCRs) ที่บังคับใช้ระหว่างบริษัทในเครือเดียวกัน บริษัทสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกันได้ เมื่อนโยบายดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงานแล้ว การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศระหว่างในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าวก็สามารถทำได้⁸³ โดยที่ไม่ต้องพิจารณาว่าต่างประเทศที่เป็นปลายทางนั้นจะมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพียงพอตามที่คณะกรรมการกำหนดหรือไม่

ทั้งนี้ การกำหนดลักษณะของผู้ประกอบธุรกิจที่อยู่ในเครือกิจการเดียวกัน หรือเครือธุรกิจเดียวกัน รวมถึงการดำเนินการจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลภายในเครือกิจการ (Binding Corporate Rules: BCRs) ให้ดำเนินการกฎหมายลำดับรองที่เกี่ยวข้อง

เพื่อเป็นข้อมูลเบื้องต้นให้แก่บริษัท ตาม GDPR เนื้อหาของ Binding Corporate Rules ควรจะมีสาระสำคัญ ดังต่อไปนี้⁸⁴

- (1) โครงสร้างของแต่ละบริษัทในเครือกิจการที่มีส่วนร่วมในการประกอบกิจการและรายละเอียดการติดต่อ
- (2) กำหนดขอบเขตของนโยบายคุ้มครองข้อมูลของบริษัทในเครือ รวมไปถึงประเภทของข้อมูลส่วนบุคคล สภาพการส่งหรือโอนข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต

⁸³ มาตรา 29 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

⁸⁴ GDPR Article 47 2 (a) – (n)

- (3) สภาพบังคับทางกฎหมายของนโยบายนี้ทั้งภายในและภายนอก
- (4) นำหลักการในการคุ้มครองข้อมูลส่วนบุคคลมาปรับใช้ โดยเฉพาะอย่างยิ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น การเก็บรักษาข้อมูลส่วนบุคคลภายในระยะเวลาจำกัด ฐานในการประมวลผลข้อมูลส่วนบุคคล (ทั้งที่ใช้สำหรับข้อมูลส่วนบุคคลทั่วไปและที่มีความอ่อนไหว) ระยะเวลาการเก็บรักษา การรักษาความปลอดภัยของข้อมูลส่วนบุคคล เป็นต้น
- (5) รับรองสิทธิและวิธีการหรือช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมไปถึงสิทธิที่จะได้รับการเยียวยาและชดเชยค่าเสียหายตามความเหมาะสม กรณีที่มีการละเมิดนโยบายนี้
- (6) ข้อตกลงความรับผิดชอบโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต่างประเทศ ที่มีความรับผิดชอบในกรณีที่ละเมิดนโยบาย เว้นเสียแต่ว่าบุคคลดังกล่าวจะพิสูจน์ได้ว่าไม่มีส่วนรับผิดชอบในเหตุที่ทำให้เกิดความเสียหาย
- (7) กระบวนการแจ้งข้อมูลเกี่ยวกับสาระสำคัญในนโยบายนี้ โดยสาระสำคัญในข้อ (4) (5) และ(6) ให้แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าตัวหรือจากแหล่งอื่น
- (8) หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หรือบุคคลที่มีหน้าที่รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ รวมไปถึงการติดตามและจัดการฝึกอบรมให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การจัดการกับข้อร้องเรียน
- (9) กระบวนการรับเรื่องร้องเรียน
- (10) กลไกในการตรวจสอบและประเมินการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลภายในเครือกิจการ เช่น การดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล การดำเนินการแก้ไขเมื่อได้รับเรื่องร้องเรียน เป็นต้น
- (11) กลไกการรายงานและบันทึกการแก้ไขเปลี่ยนแปลงของนโยบายนี้ โดยต้องรายงานการเปลี่ยนแปลงดังกล่าวให้แก่หน่วยงานกำกับดูแล
- (12) กำหนดกลไกในการให้ความร่วมมือกับหน่วยงานกำกับดูแล เพื่อให้แน่ใจว่าได้มีการปฏิบัติตามนโยบาย โดยเฉพาะอย่างยิ่งการเปิดเผยผลตรวจสอบในข้อ (10)
- (13) กลไกในการรายงานต่อหน่วยงานกำกับดูแลที่มีอำนาจเกี่ยวกับหน้าที่ตามกฎหมายใด ๆ ที่บริษัทในเครือจะต้องปฏิบัติตามในต่างประเทศ โดยที่หน้าที่ดังกล่าวอาจมีผลกระทบต่อการรับรองและการตกลงต่าง ๆ ในนโยบายนี้ และ

(14) จัดการฝึกอบรมให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมแก่พนักงานที่สามารถเข้าถึงข้อมูลส่วนบุคคล ไม่ว่าจะมีความสามารถเข้าถึงได้อย่างถาวรหรือเป็นครั้งคราวก็ตาม

ทั้งนี้ บริษัทควรเก็บบันทึกการเข้าถึงและการใช้ข้อมูลส่วนบุคคลของบริษัทในเครือ ตลอดจนติดตามตรวจสอบความเหมาะสมในการใช้งานข้อมูลส่วนบุคคลตามนโยบายข้างต้น เช่น ตรวจสอบให้แน่ใจว่าบริษัทได้ลบหรือทำลายข้อมูลส่วนบุคคลอย่างเหมาะสมแล้วภายหลังจากที่บริษัทไม่มีความจำเป็นที่จะต้องใช้งานหรือครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าว เป็นต้น

6.4 ข้อยกเว้นอื่น

ในกรณีที่บริษัทยังไม่มีกำหนด**มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ** หรือยังไม่มีนโยบายภายในเครือบริษัท บริษัทยังสามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศได้ โดยไม่ต้องปฏิบัติตามหลักการข้างต้น หากบริษัทมีมาตรการคุ้มครองที่เหมาะสมที่สามารถบังคับได้ตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีที่มีการใช้สิทธิ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ทั้งนี้ หากเทียบแนวทางจากหลักการของ GDPR ในกรณีที่ประเทศปลายทาง หรือองค์กรปลายทางไม่มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจดำเนินการอื่นที่มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมได้ โดยนอกจากจะมีการใช้ Binding Corporate Rules แล้ว บริษัทยังสามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศให้กับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอื่น โดยการเข้าทำสัญญาซึ่งมีการกำหนดเงื่อนไขเกี่ยวกับการโอนข้อมูลส่วนบุคคล การปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมถึงการให้เจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการตามสิทธิของตน และมีมาตรการเยียวยาเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลได้

ในกรณีดังกล่าวนี้ ในต่างประเทศได้มีการออกข้อสัญญามาตรฐานในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในกรณีที่ประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ปฏิบัติตามด้วย โดยสัญญาดังกล่าวอย่างน้อยควรประกอบไปด้วยข้อสัญญาในเรื่องดังต่อไปนี้⁸⁵

1. รายละเอียดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ได้แก่ ประเภทของข้อมูลส่วนบุคคลที่จะมีการโอนไปยังต่างประเทศ โดยเฉพาะอย่างยิ่งหากมีการโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังต่างประเทศ จะต้องระบุในสัญญา หรือแนบท้ายสัญญาด้วย
2. การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงการกำหนดในเรื่องสิทธิในการร้องเรียน หรือฟ้องร้องต่อผู้ส่งข้อมูลส่วนบุคคล และผู้รับข้อมูลส่วนบุคคล
3. การกำหนดหน้าที่ของผู้ส่งข้อมูลส่วนบุคคลไปยังต่างประเทศ เช่น หน้าที่ในการจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
4. การกำหนดหน้าที่ของผู้รับข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ
5. ความรับผิดชอบของผู้ส่งข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล

⁸⁵ International Transfer, ICO, <https://ico.org.uk/media/2553982/ico-guidance-controller-to-controller.docx>, accessed on 24 April 2020

6. กำหนดกฎหมายที่ใช้บังคับ และวิธีการในการระงับข้อพิพาท

นอกจากการเข้าทำสัญญาตามข้อสัญญามาตรฐานที่มีการควบคุมการคุ้มครองข้อมูลส่วนบุคคลระหว่างผู้โอน และผู้รับโอนข้อมูลส่วนบุคคลแล้ว ตาม GDPR ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยการที่ให้ผู้รับโอนข้อมูลส่วนบุคคลลงนามในหลักเกณฑ์การปฏิบัติ (Code of Conduct) ของผู้โอนข้อมูลส่วนบุคคล และดำเนินการให้หน่วยงานที่เกี่ยวข้องรับรอง Code of Conduct นั้น ๆ ได้⁸⁶

ข้อสังเกต

- การโอนข้อมูลนิรนามไปนอกประเทศ: หากข้อมูลส่วนบุคคลได้ผ่านกระบวนการทำให้เป็นข้อมูลนิรนาม (Anonymized Data) แล้ว โดยผู้รับไม่สามารถระบุตัวตนได้ ข้อมูลดังกล่าวขาดสถานะความเป็นข้อมูลส่วนบุคคลไปตั้งแต่ตอนที่ผ่านกระบวนการทำให้เป็นข้อมูลนิรนามไปแล้ว ดังนั้น การส่งหรือโอนข้อมูลนั้น จึงไม่ถือว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ
- การส่งผ่านข้อมูล: กรณีที่มีการส่งผ่านข้อมูลส่วนบุคคลภายในประเทศไทย โดยที่ข้อมูลส่วนบุคคลถูกส่งผ่านไปยังเซิร์ฟเวอร์ในต่างประเทศโดยตรง (อาทิ ประเทศสิงคโปร์) ก่อนที่จะกลับมายังประเทศไทยอีกครั้งหนึ่ง ในกรณีนี้การส่งผ่านข้อมูลส่วนบุคคลดังกล่าว ไม่ถือว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ
- การนำส่งข้อมูลไปยังเว็บไซต์ต่างประเทศ: เมื่อผู้ควบคุมข้อมูลส่วนบุคคลนำส่ง (Upload) ข้อมูลส่วนบุคคลไปยังเว็บไซต์ในต่างประเทศ โดยสามารถคาดได้ว่าเว็บไซต์ดังกล่าวนั้นมีเซิร์ฟเวอร์ (Server) ตั้งอยู่ในต่างประเทศ การนำส่งข้อมูลส่วนบุคคลดังกล่าวถือเป็นการส่งหรือโอนข้อมูลไปยังปลายทางต่างประเทศ เช่นเดียวกับการใช้ระบบ Cloud ที่มีเซิร์ฟเวอร์ตั้งอยู่ในต่างประเทศ

⁸⁶ International Transfer, ICO, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/>, accessed on 24 April 2020.

บทที่ 7 แนวทางการปฏิบัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของตน โดยอาจสรุปได้ดังต่อไปนี้

- 1) สิทธิในการเพิกถอนความยินยอม (Right to Withdraw Consent)
- 2) สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)
- 3) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access)
- 4) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification)
- 5) สิทธิในการลบข้อมูลส่วนบุคคล (Right to Erasure)
- 6) สิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคล (Right to Restriction of Processing)
- 7) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability)
- 8) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object)
- 9) สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ (Right to Lodge a Complaint)

ข้อสังเกต

นอกจากสิทธิข้างต้นที่ได้มีการรับรองไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แล้ว GDPR ยังรับรองสิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (Right not to be Subject to Automated Individual Decision-Making, including Profiling) ไว้อีกด้วย

ในส่วนนี้แนวปฏิบัติฉบับนี้จะอธิบายเนื้อหาและขอบเขตของสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลรับรองข้างต้น รวมถึงแนวทางปฏิบัติของบริษัท เมื่อมีการร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล ต่อไปเป็นลำดับ เพื่อให้บริษัทสามารถเตรียมพร้อมปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้อย่างเหมาะสม

7.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล

7.1.1 สิทธิในการเพิกถอนความยินยอม (Right to Withdraw Consent)⁸⁷

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะถอนความยินยอมเมื่อใดก็ได้ โดยร้องขอกับผู้ควบคุมข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 19 ทั้งนี้ กระบวนการใช้สิทธิเพิกถอนความยินยอมข้างต้นจะต้องทำได้โดยง่ายเหมือนกับการให้ความยินยอม ดังนั้น บริษัทจึงอาจจะจัดเตรียมช่องทางที่สะดวกต่อการเข้าถึงได้ง่าย เพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิเพิกถอนความยินยอม เช่น การใช้สิทธิเพิกถอนผ่านเว็บไซต์ อีเมล หรือ Call Center เป็นต้น

ทั้งนี้ เมื่อบริษัทได้รับคำร้องขอเพิกถอนความยินยอมข้างต้นจากเจ้าของข้อมูลส่วนบุคคลแล้ว บริษัทควรจะต้องดำเนินการ ดังต่อไปนี้

1. แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบของการเพิกถอนความยินยอม
2. ค้นหาและแยกข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมาโดยอาศัยฐานความยินยอม
3. หยุดประมวลผลข้อมูลส่วนบุคคลที่อาศัยฐานความยินยอม โดยไม่ล่าช้า นับแต่ทราบถึงการร้องขอใช้สิทธิเพิกถอนความยินยอมนั้น เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงฐานในการประมวลผลข้อมูลฐานอื่นนอกจากฐานความยินยอมได้

การปฏิเสธคำขอ

บริษัทอาจปฏิเสธคำขอเพิกถอนความยินยอมได้ ในกรณีดังต่อไปนี้

1. มีข้อกำหนดสิทธิในการถอนความยินยอมตามกฎหมาย หรือ
2. มีข้อกำหนดสิทธิในการถอนความยินยอมตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ข้อสังเกต

- ข้อมูลส่วนบุคคลที่ได้ถูกประมวลผลไปแล้วโดยชอบด้วยกฎหมาย ก่อนที่เจ้าของข้อมูลส่วนบุคคลจะร้องขอใช้สิทธิในการเพิกถอนความยินยอมต่อผู้ควบคุมข้อมูลส่วนบุคคล ไม่ถูกกระทบกระเทือน
- ภายหลังหรือขณะที่เพิกถอนความยินยอม หากเจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ ตาม

⁸⁷ มาตรา 19 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 33 บริษัทต้องดำเนินการลบหรือทำลาย ตามคำขอข้างต้นด้วย เว้นแต่ ได้รับยกเว้นตามกฎหมาย

- ในการจัดเตรียมช่องทางเพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิเพิกถอนความยินยอม บริษัทควรออกแบบให้เจ้าของข้อมูลส่วนบุคคลสามารถเลือกใช้สิทธิเพิกถอนความยินยอม เป็นรายกรณี หรือรายวัตถุประสงค์ไป เพื่อไม่ให้ถูกเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมาทั้งหมด เช่น บริษัทควรขอความยินยอมเพื่อดำเนินการทำการตลาดของบริษัทเอง แยกกับการขอความยินยอมในการดำเนินการตลาด หรือการเสนอขายผลิตภัณฑ์ของคู่ค้าของบริษัท เช่น ผลิตภัณฑ์ของธนาคาร เป็นต้น

หมายเหตุ

การประมวลผลข้อมูลส่วนบุคคลเพื่อการเสนอขายผลิตภัณฑ์ของบริษัทเองให้แก่ลูกค้าเดิมของบริษัท อาจอ้างอิงฐานประโยชน์อันชอบธรรมได้ ไม่จำเป็นต้องขอความยินยอม

7.1.2 สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)⁸⁸

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการได้รับแจ้งข้อมูล (Right to be informed) โดยที่ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งรายละเอียด ต่อไปนี้

1. แจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ก่อนหรือขณะขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
2. แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอม ในกรณีที่เจ้าของข้อมูลส่วนบุคคลขอถอนความยินยอม
3. แจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลใหม่ กรณีมีการเปลี่ยนแปลงวัตถุประสงค์
4. แจ้งรายละเอียดตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 23 กำหนด ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว
5. แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 25

⁸⁸ มาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

6. แจ้งเหตุละเมิดข้อมูลส่วนบุคคล พร้อมกับแนวทางการเยียวยาให้เจ้าของข้อมูลส่วนบุคคลทราบ ในกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล
7. แจ้งรายละเอียดเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีติดต่อ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อสอบถามเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้

ข้อสังเกต

สิทธิในการได้รับแจ้งข้อมูลนี้ เจ้าของข้อมูลส่วนบุคคล ไม่จำเป็นต้องร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิ เพราะกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องแจ้งรายละเอียดข้างต้นอยู่แล้ว

7.1.3 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access)⁸⁹

สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สามารถแบ่งออกได้ ดังนี้

1. สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของบริษัท
2. สิทธิขอให้เปิดเผยแหล่งที่มาของข้อมูลส่วนบุคคลของตนที่เจ้าของข้อมูลส่วนบุคคลไม่ได้เป็นผู้ให้ความยินยอมได้

ในการดำเนินการตามสิทธิในการเข้าถึงข้อมูลส่วนบุคคลนี้ คณะกรรมการอาจมีการประกาศกำหนดหลักเกณฑ์เกี่ยวกับการขอเข้าถึงและรับสำเนาข้อมูลส่วนบุคคลออกมา

ทั้งนี้ ตามแนวทางของ GDPR⁹⁰ เมื่อมีการร้องขอใช้สิทธิ บริษัทควรจัดให้มีเอกสาร หรือรายละเอียดดังต่อไปนี้

- สำเนาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลนั้น
- วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- ประเภทของข้อมูลส่วนบุคคล
- ผู้ที่ได้รับการเปิดเผยข้อมูลส่วนบุคคล หรือประเภทของบุคคลดังกล่าว

⁸⁹ มาตรา 30 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

⁹⁰ Right of Access, GDPR, <https://gdpr-info.eu/issues/right-of-access/>, accessed on 24 April 2020.

- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล หรือหลักเกณฑ์ในการกำหนดระยะเวลาเก็บรักษา ดังกล่าว
- สิทธิในการแก้ไขข้อมูลส่วนบุคคล ลบข้อมูลส่วนบุคคล หรือห้ามหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคล
- สิทธิในการยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล
- แหล่งที่มาของข้อมูลส่วนบุคคล ที่ได้มาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล
- การตัดสินใจอัตโนมัติ (Automation) และโปรไฟล์ลิ่ง (Profiling)
- มาตรการรักษาความมั่นคงปลอดภัย ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังปลายทางต่างประเทศ

กรอบระยะเวลาในการดำเนินการตามสิทธิ

บริษัทจะต้องดำเนินการตามคำขอข้างต้นของเจ้าของข้อมูลส่วนบุคคล ไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอดังกล่าว หากไม่มีข้ออ้างที่จะเป็นเหตุในการปฏิเสธการปฏิบัติตามคำขอดังกล่าวได้ ทั้งนี้ กรอบระยะเวลานี้ อาจขยายได้ตามประกาศของคณะกรรมการ

การปฏิเสธคำขอ

บริษัทอาจปฏิเสธไม่ปฏิบัติตามคำขอใช้สิทธิข้างต้นของเจ้าของข้อมูลส่วนบุคคลได้ในเฉพาะกรณีดังต่อไปนี้

1. เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล
2. การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลดังกล่าวจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่นได้

เมื่อ บริษัทได้ปฏิเสธคำขอข้างต้นแล้ว บริษัทจะต้องบันทึกรายละเอียดการปฏิเสธคำขอข้างต้นพร้อมเหตุผลไว้ ตามรายการที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย

ข้อสังเกต

- กฎหมายไม่ได้กำหนดแบบในการขอใช้สิทธินี้ไว้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงอาจขอใช้สิทธิ โดยการร้องขอเป็นหนังสือหรือด้วยวาจาก็ได้ ซึ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิ เป็นหนังสือ บริษัทควรจัดเตรียมแบบฟอร์มการขอใช้สิทธิ แต่หากกรณีที่เจ้าของข้อมูลส่วนบุคคล ร้องขอใช้สิทธิด้วยวาจา บริษัทควรจะบันทึกเสียงเพื่อเก็บไว้เป็นหลักฐาน รายละเอียดตามข้อ 7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- การดำเนินการที่เกี่ยวกับการดำเนินการตามสิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลให้เป็นไปตาม กฎหมายลำดับรอง

ข้อพิจารณาเบื้องต้น

บริษัทควรดำเนินการดังต่อไปนี้

- จัดเตรียมบันทึกเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามรายละเอียดข้างต้น
- ระบุถึงกฎหมายหรือคำสั่งศาลที่จะเป็นเหตุในการปฏิเสธคำขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (หากมี)

7.1.4 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification)⁹¹

การประมวลผลข้อมูลส่วนบุคคลนั้น ควรจะต้องทำการประมวลผลข้อมูลที่ถูกต้อง เป็นปัจจุบัน สมบูรณ์ เพื่อให้บรรลุตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลได้อย่างแม่นยำและถูกต้อง โดยไม่ ก่อให้เกิดความเข้าใจผิด ซึ่งจะช่วยลดความเสี่ยงและผลกระทบที่อาจทำให้เกิดความเสียหายแก่เจ้าของข้อมูล ส่วนบุคคลหรือบุคคลอื่นได้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิดได้ ตามหลักการ ประมวลข้อมูลส่วนบุคคลอย่างถูกต้อง (Accuracy Principle) ของ GDPR⁹² และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

หากบริษัทปฏิเสธไม่ดำเนินการตามคำร้องขอให้แก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง บริษัทจะต้องบันทึก รายละเอียดการปฏิเสธคำร้องขอข้างต้นพร้อมเหตุผลไว้ ตามรายการที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย

⁹¹ มาตรา 35 และมาตรา 36 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

⁹² Article 5(1)(d) of the GDPR

ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลบริษัทถูกปฏิเสธข้างต้น เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้อีกด้วย

ข้อสังเกต

- สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องนี้ เจ้าของข้อมูลส่วนบุคคลคนนั้น ไม่จำเป็นต้องร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิ เพราะกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด อยู่แล้ว
- ข้อมูลที่ไม่ถูกต้อง (Inaccurate) คือ ข้อมูลที่ไม่ตรงกับความเป็นจริง
- ข้อมูลที่ไม่สมบูรณ์ (Incomplete) คือ ข้อมูลที่ถูกต้องตรงกับความเป็นจริง แต่ไม่ครบถ้วนสมบูรณ์
- กฎหมายไม่ได้กำหนดแบบในการขอใช้สิทธินี้ไว้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงอาจขอใช้สิทธิโดยการร้องขอเป็นหนังสือหรือด้วยวาจาก็ได้ ซึ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิเป็นหนังสือ บริษัทควรจัดเตรียมแบบฟอร์มการขอใช้สิทธิ แต่หากกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิด้วยวาจา บริษัทควรจะบันทึกเสียงเพื่อเก็บไว้เป็นหลักฐาน รายละเอียดตามข้อ 7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- กรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก บริษัทต้องแจ้งให้บุคคลดังกล่าวแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลนั้นให้ถูกต้องสมบูรณ์ด้วย
- บริษัทต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงสิทธิข้างต้น โดยระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลด้วย

ข้อแนะนำ

- บริษัทควรหยุดการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้แก้ไขไว้ชั่วคราวก่อน ไม่ว่าเจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิในการคัดค้านหรือห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลแล้วหรือไม่ก็ตาม เพราะหากบริษัททำการประมวลผลข้อมูลส่วนบุคคลนั้นต่อ ก็อาจทำให้เกิดความเข้าใจผิดและอาจเสียหายได้
- บริษัทอาจขอหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อประกอบการพิจารณาและพิสูจน์ความไม่ถูกต้องของข้อมูลส่วนบุคคลได้ ตามที่เจ้าของข้อมูลส่วนบุคคลกล่าวอ้าง เช่น เอกสารที่ออกโดยหน่วยงานราชการ เป็นต้น

- บริษัทควรบันทึกกระบวนการตรวจสอบความถูกต้องและแก้ไขข้อมูลส่วนบุคคลไว้ แต่ห้ามนำข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ไม่เป็นปัจจุบัน หรือไม่สมบูรณ์มาใช้
- บริษัทควรบันทึกกระบวนการแก้ไขหรือตรวจสอบข้อมูลส่วนบุคคลนั้นไว้เสมอไม่ว่าจะมีการแก้ไขข้อมูลส่วนบุคคลตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม เพื่อเป็นหลักฐานว่าบริษัทได้ดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายแล้ว โดยบริษัทอาจบันทึกทั้งข้อมูลเดิม หลักฐานที่ใช้พิสูจน์ ข้อมูลที่แก้ไข เหตุผลในการปฏิเสธการใช้สิทธิ เป็นต้น

7.1.5 สิทธิในการลบข้อมูลส่วนบุคคล (Right to be Forgotten)⁹³

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล (De-identification) ได้ ในกรณีดังต่อไปนี้

1. เมื่อข้อมูลส่วนบุคคลไม่มีความจำเป็นในการเก็บรักษาไว้เพื่อประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อีกต่อไป
2. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างอิงฐานในการประมวลผลข้อมูลฐานอื่น นอกจากฐานความยินยอมได้
3. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลโดยอ้างอิงฐานปฏิบัติตามกฎหมาย หรือฐานประโยชน์อันชอบธรรม แต่ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถพิสูจน์ได้ว่า
 - 3.1 ในการประมวลผลข้อมูลส่วนบุคคลดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
 - 3.2 การประมวลผลข้อมูลส่วนบุคคลดังกล่าว เป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย
 - 3.3 การประมวลผลข้อมูลส่วนบุคคลดังกล่าวเป็นไปเพื่อการปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย
 - 3.4 การประมวลผลข้อมูลส่วนบุคคลดังกล่าวเป็นไปเพื่อการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

⁹³ มาตรา 33 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

4. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

5. เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผล โดยไม่ชอบด้วยกฎหมาย

ในกรณีที่ข้อมูลส่วนบุคคลกลายเป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยการกระทำของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลคนนั้นจะต้องเป็นผู้รับผิดชอบโดยดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอใช้สิทธิในการลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล พร้อมทั้งแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ

เหตุในการปฏิเสธ

1. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
2. การเก็บรักษาไว้เพื่อวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (1)
3. การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอธิปไตยได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (4)
4. การเก็บรักษาข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษไว้เพื่อวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 (5) (ก)
5. การเก็บรักษาข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษไว้เพื่อวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 (5) (ข)
6. ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุในการปฏิเสธคำขอใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ก) หรือ(ข)
7. การใช้เพื่อวัตถุประสงค์ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
8. การใช้เพื่อวัตถุประสงค์ในการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
9. การใช้เพื่อวัตถุประสงค์ในการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

10. การปฏิบัติตามกฎหมาย

อย่างไรก็ตาม เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในเรื่องเกี่ยวกับการดำเนินการตามสิทธิ เช่น กรณีที่เจ้าของข้อมูลส่วนบุคคลไม่เห็นด้วยกับการดำเนินการของบริษัท

ข้อสังเกต

- กฎหมายไม่ได้กำหนดแบบในการขอใช้สิทธินี้ไว้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงอาจขอใช้สิทธิโดยการร้องขอเป็นหนังสือหรือด้วยวาจาก็ได้ ซึ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิเป็นหนังสือ บริษัทควรจัดเตรียมแบบฟอร์มการขอใช้สิทธิ แต่หากกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิด้วยวาจา บริษัทควรจะบันทึกเสียงเพื่อเก็บไว้เป็นหลักฐาน รายละเอียดตามข้อ 7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- การลบ หรือทำลายข้อมูลส่วนบุคคล อาจทำได้โดยทำให้ข้อมูลดังกล่าวไม่สามารถอ่านได้ หรือไม่สามารถประมวลผลข้อมูลได้ หรือไม่สามารถนำกลับมาใช้ได้อีก โดยการดำเนินการดังกล่าวให้เป็นไปตามกฎหมายลำดับรอง
- กฎหมายไม่ได้ระบุโดยเฉพาะเจาะจงให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแบบใด ดังนั้น หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ระบุให้บริษัทดำเนินการอย่างใดอย่างหนึ่งโดยเฉพาะเจาะจง บริษัทอาจมีดุลพินิจเลือกดำเนินการระหว่าง การลบ การทำลาย และการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นก็ได้
- บริษัทมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงสิทธิข้างต้น โดยระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลด้วย

ข้อแนะนำ

- บริษัทควรตรวจสอบวิธีการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่ให้สอดคล้องกับกฎหมายลำดับรองเสมอ
- บริษัทควรใช้ถ้อยคำในแบบคำร้องที่มีลักษณะเป็นคำขอแบบกว้างๆ เช่น “ข้าพเจ้ามีความประสงค์ให้บริษัทดำเนินการตามคำร้องขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล...” ทั้งนี้ เพื่อให้บริษัทเป็นฝ่ายที่จะสามารถเลือกวิธีการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เนื่องจากคำร้องไม่ได้ระบุให้บริษัทจะต้องดำเนินการอย่างใดอย่างหนึ่งโดยเฉพาะ

7.1.6 สิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคล (Right to Restrict Processing)⁹⁴

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

1. เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 36
2. เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลาย เพราะเป็นข้อมูลส่วนบุคคลที่ถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้แทน
3. เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมของผู้ควบคุมข้อมูลส่วนบุคคลแล้ว แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อวัตถุประสงค์ดังต่อไปนี้
 - เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
 - เพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
 - เพื่อการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
4. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า เป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐหรือฐานประโยชน์อันชอบธรรม หรือเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ก)
5. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า เป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐหรือฐานประโยชน์อันชอบธรรม หรือเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ข) เพื่อวัตถุประสงค์ดังต่อไปนี้
 - เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
 - เพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย

⁹⁴ มาตรา 34 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- เพื่อการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
6. เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า เป็นการประมวลผลข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ที่เป็นไปเพื่อความจำเป็นในการดำเนินการกิจการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

การปฏิเสธคำขอ

1. กรณีที่บริษัทพิสูจน์ได้ว่าข้อมูลส่วนบุคคลที่มีอยู่ถูกต้อง สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
2. กรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิระงับการประมวลผลข้อมูลส่วนบุคคล โดยอ้างว่าบริษัท ไม่มีความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมของผู้ควบคุมข้อมูลส่วนบุคคลแล้ว แต่บริษัทสามารถพิสูจน์ได้ว่า บริษัทยังมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลอยู่
3. กรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิระงับการประมวลผลข้อมูลส่วนบุคคล โดยยังไม่ได้ใช้สิทธิคัดค้านการประมวลผลข้อมูล (บริษัทจะต้องมั่นใจว่า บริษัทสามารถพิสูจน์โดยเข้าข้อยกเว้น หรือเหตุปฏิเสธที่จะไม่ปฏิบัติตามสิทธิคัดค้านการประมวลผลข้อมูลเสียก่อนที่จะอ้างเหตุปฏิเสธนี้)

ทั้งนี้ หากบริษัทปฏิเสธคำขอใช้สิทธิข้างต้น บริษัทจะต้องบันทึกการปฏิเสธคำขอ พร้อมด้วยเหตุผลไว้ในรายการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย

ข้อสังเกต

- กฎหมายไม่ได้กำหนดแบบในการขอใช้สิทธินี้ไว้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงอาจขอใช้สิทธิโดยการร้องขอเป็นหนังสือหรือด้วยวาจาก็ได้ ซึ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิเป็นหนังสือ บริษัทควรจัดเตรียมแบบฟอร์มการขอใช้สิทธิ แต่หากกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิด้วยวาจา บริษัทควรจะบันทึกเสียงเพื่อเก็บไว้เป็นหลักฐาน รายละเอียดตามข้อ 7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- หากบริษัทได้เปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอกไปแล้วก่อนที่จะมีการร้องขอใช้สิทธิห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล บริษัทควรแจ้งให้บุคคลภายนอกดังกล่าวทราบถึงการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย

- ตามที่ได้อธิบายข้างต้น จะสังเกตได้ว่าสิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลนี้ ในหลายกรณีจะมีเงื่อนไขในการใช้สิทธิ กล่าวคือ เจ้าของข้อมูลส่วนบุคคลจะต้องใช้สิทธิอื่น ๆ เสียก่อน (เช่น สิทธิคัดค้านการประมวลผลข้อมูล สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นต้น) และผู้ควบคุมข้อมูลส่วนบุคคลอ้างว่าอยู่ในระหว่างตรวจสอบการใช้สิทธิดังกล่าวแล้ว เจ้าของข้อมูลส่วนบุคคลจึงจะสามารถร้องขอใช้สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลได้ต่อไป
- บริษัทจะดำเนินการตามสิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคลนี้ได้ เมื่อมีการร้องขอ กล่าวคือ ถ้าเจ้าของข้อมูลไม่ร้องขอ บริษัทก็ไม่จำเป็นต้องดำเนินการตามสิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคล แม้ว่าบริษัทกำลังอยู่ในการตรวจสอบการใช้สิทธิอื่น ๆ (เช่น สิทธิคัดค้านการประมวลผลข้อมูล สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นต้น) ที่เป็นเงื่อนไขในการใช้สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลก็ตาม
- บริษัทต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงสิทธิข้างต้น โดยระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลด้วย
- การดำเนินการเกี่ยวกับการใช้สิทธิ และการปฏิบัติตามสิทธิให้เป็นไปตามกฎหมายลำดับรอง

ข้อแนะนำ

- บริษัท อาจจะดำเนินการดังต่อไปนี้ เพื่อระงับการใช้ข้อมูลส่วนบุคคลตามคำร้องขอใช้สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
 - แยกข้อมูลส่วนบุคคลนั้นไปไว้ที่ระบบเก็บรักษาข้อมูล ที่ไม่มีการประมวลผลข้อมูลซ้ำคราว
 - จำกัดการเข้าถึงข้อมูลส่วนบุคคลนั้นซ้ำคราว
 - หยุดการประมวลผลเฉพาะข้อมูลส่วนบุคคลนั้นไว้ซ้ำคราว
- บริษัท ควรทบทวนวิธีการระงับใช้ข้อมูลส่วนบุคคลของบริษัท ให้สอดคล้องกับกฎหมายลำดับรองอยู่เสมอ

7.1.7 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability)⁹⁵

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้โอนย้ายข้อมูลส่วนบุคคลได้ โดยมีเงื่อนไขดังต่อไปนี้

1. ประเภทข้อมูลส่วนบุคคลที่สามารถร้องขอให้โอนได้
 - 1.1 ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอม ในการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
 - 1.2 ข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม เพราะเป็นข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมไว้เพื่อความจำเป็นในการประมวลผลข้อมูล ในฐานะสัญญาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมาตรา 24 (3)
 - 1.3 ข้อมูลส่วนบุคคลอื่นที่กำหนด ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 ตามที่คณะกรรมการประกาศกำหนด (ซึ่งปัจจุบัน คณะกรรมการยังไม่ได้ประกาศกำหนด)

ตัวอย่าง

- ผู้เอาประกันภัยมีสิทธิร้องขอให้บริษัทหนึ่งโอนข้อมูลส่วนบุคคลของตนไปยังอีกบริษัท หนึ่งได้
- ผู้เอาประกันภัยมีสิทธิร้องขอให้บริษัทโอนข้อมูลส่วนบุคคลของตนไปยังบริษัทนายหน้าประกันภัย

⁹⁵ มาตรา 31 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- ผู้เอาประกันภัยมีสิทธิร้องขอให้บริษัทโอนข้อมูลส่วนบุคคลของตนไปยังโรงพยาบาลที่ผู้เอาประกันภัยรักษาอยู่

2. ต้องเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลในข้อ 1 ประเภทข้อมูลส่วนบุคคลที่สามารถร้องขอให้โอนได้ ข้างต้นนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

โดยสิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล ที่เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้ มีดังต่อไปนี้

- ก. ขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้
- ข. ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น เมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
- ค. ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบ ดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

หากบริษัทปฏิเสธไม่ดำเนินการตามคำร้องขอให้โอนย้ายข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลข้างต้นนี้ บริษัทจะต้องบันทึกรายละเอียดการปฏิเสธคำขอข้างต้นพร้อมเหตุผลไว้ ตามรายการที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย

การปฏิเสธคำขอ

1. ไม่ใช่ข้อมูลส่วนบุคคลตามเงื่อนไขข้อ 1 ข้างต้น
2. การส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ เช่น กรณีที่ ปปง. เป็นผู้ควบคุมข้อมูลส่วนบุคคลทำการส่งหรือโอนข้อมูลส่วนบุคคลไปยังสำนักงานตำรวจแห่งชาติเพื่อป้องกันและปราบปรามการฟอกเงิน
3. การส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่ตามกฎหมาย เช่น กรณีที่บริษัท ผู้ควบคุมข้อมูลส่วนบุคคลทำการส่งหรือโอนข้อมูลส่วนบุคคลไปยังสำนักงาน คปภ. เพื่อปฏิบัติตามประกาศของสำนักงาน คปภ.
4. การใช้สิทธิข้างต้นนั้น ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น

ข้อสังเกต

ประเภทข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอใช้สิทธิในการโอนย้ายข้อมูลข้างต้น อาจตีความให้รวมไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เก็บรวบรวมมาโดยอาศัยความยินยอมโดยชัดแจ้ง ได้ แต่ไม่รวม ข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ได้รับการยกเว้นให้ไม่ต้องขอความยินยอมโดยชัดแจ้ง ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 26

7.1.8 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object)⁹⁶

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ในกรณีดังต่อไปนี้

1. กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมในกรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า
 - 1.1. การประมวลผลข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
 - 1.2. การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อ
 - ก่อตั้งสิทธิเรียกร้องตามกฎหมาย
 - การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
 - การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
2. กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
3. กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับ การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจ เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

⁹⁶ มาตรา 32 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

การปฏิเสธคำขอ

1. กรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ก)
2. กรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลภายใต้วัตถุประสงค์ ดังต่อไปนี้ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ข)
 - เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
 - เพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย
 - เพื่อการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
3. กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ที่เป็นไปเพื่อความจำเป็นในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (3)

อนึ่ง หากบริษัทปฏิเสธไม่ดำเนินการตามคำขอคัดค้านการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลข้างต้นนี้ บริษัทจะต้องบันทึกรายละเอียดการปฏิเสธคำขอข้างต้นพร้อมเหตุผลไว้ ตามรายการที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 39 กำหนดด้วย

ข้อสังเกต

- บริษัทไม่สามารถอ้างเหตุในการปฏิเสธได้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิคัดค้านการประมวลผลข้อมูลข้างต้น ไม่ว่าจะเกิดเหตุในการปฏิเสธหรือไม่ก็ตาม บริษัทจะต้องแยกข้อมูลส่วนบุคคลดังกล่าวออกจากระบบประมวลผลข้อมูลปกติและเก็บรักษาไว้ในฐานข้อมูลส่วนบุคคลที่ไม่มีการประมวลผลข้อมูลก่อนทันที เพื่อป้องกันไม่ให้มีการประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
- บริษัทจะดำเนินการตามสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลนี้ได้ ต้องมีการร้องขอกล่าวคือ ถ้าเจ้าของข้อมูลไม่ร้องขอ บริษัทก็ไม่จำเป็นต้องดำเนินการตามสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

- ถ้อยคำตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (3) ที่กำหนดให้เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลใน “(๓) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ...” นั้น สอดคล้องกับฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 (5) (ง) จึงอาจเป็นกรณีที่สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลสำหรับกรณีนี้ จำกัดอยู่เพียงการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว
- กฎหมายไม่ได้กำหนดแบบในการขอใช้สิทธินี้ไว้ ดังนั้น เจ้าของข้อมูลส่วนบุคคลจึงอาจขอใช้สิทธิ โดยการร้องขอเป็นหนังสือหรือด้วยวาจาก็ได้ ซึ่งในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิ เป็นหนังสือ บริษัทควรจัดเตรียมแบบฟอร์มการขอใช้สิทธิ แต่หากกรณีที่เจ้าของข้อมูลส่วนบุคคล ร้องขอใช้สิทธิด้วยวาจา บริษัทควรจะบันทึกเสียงเพื่อเก็บไว้เป็นหลักฐาน รายละเอียดตามข้อ 7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- บริษัทควรจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงสิทธิข้างต้น โดยระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลด้วย

7.1.9 สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ (Right to Lodge a Complaint)⁹⁷

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ในกรณีที่มิฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือประกาศที่ออกตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยบุคคล ดังต่อไปนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคล
2. ผู้ประมวลผลข้อมูลส่วนบุคคล
3. ลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4. ผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

เมื่อคณะกรรมการผู้เชี่ยวชาญรับเรื่องแล้ว คณะกรรมการผู้เชี่ยวชาญจะพยายามไกล่เกลี่ยก่อน โดยถ้าหากเรื่องร้องเรียนนั้นไม่สามารถไกล่เกลี่ยได้ หรือไกล่เกลี่ยไม่สำเร็จนั้น คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่งได้ 3 กรณี ดังนี้

⁹⁷ มาตรา 72-74 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

1. สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด
2. สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล
3. สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในการพิจารณาเรื่องร้องเรียน คณะกรรมการผู้เชี่ยวชาญ ที่มีอำนาจและหน้าที่ในการพิจารณาเรื่องร้องเรียน สามารถเรียกให้บุคคลใด ๆ มาชี้แจงข้อเท็จจริง หรือสั่งให้บุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดที่เกี่ยวข้องการคุ้มครองข้อมูลส่วนบุคคลได้ รวมทั้งจะสั่งให้บุคคลมาชี้แจงข้อเท็จจริงได้

ทั้งนี้ ขั้นตอนการยื่น การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาเรื่องร้องเรียนให้เป็นไปตามกฎหมายลำดับรอง

ข้อสังเกต

- คำสั่งห้ามกระทำการที่ก่อให้เกิดความเสียหายนั้น อาจเป็นกรณีที่เป็นการสั่งก่อนที่จะมีความเสียหายเกิดขึ้น (กล่าวคือ ยังไม่มีความเสียหายแต่น่าจะเกิดความเสียหาย) หรือที่มีความเสียหายเกิดขึ้นแล้วก็ได้
- คำสั่งให้ระงับความเสียหาย (Mitigate Loss) นั้น จะต้องมีความเสียหายเกิดขึ้นแล้ว จึงจะทำการระงับความเสียหายนั้นได้ คณะกรรมการผู้เชี่ยวชาญจะออกคำสั่งโดยที่ยังไม่มีความเสียหายเกิดขึ้นก่อนไม่ได้
- คำสั่งของคณะกรรมการผู้เชี่ยวชาญในกรณีนี้เป็นคำสั่งทางปกครอง จึงสามารถอุทธรณ์คำสั่งต่อศาลปกครองต่อไปได้ตามกฎหมายว่าด้วยการจัดตั้งและวิธีพิจารณาคดีปกครอง

7.2 แนวทางปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ โดยกำหนดรายละเอียดเงื่อนไขการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและเหตุแห่งการปฏิเสธดำเนินการตามสิทธิเอาไว้ แต่ไม่ได้วางหลักการหรือแนวทางขั้นตอนในการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล ดังนั้น แนวทางปฏิบัติฉบับนี้จึงขอเสนอแนวทางเบื้องต้นเกี่ยวกับขั้นตอนที่บริษัท

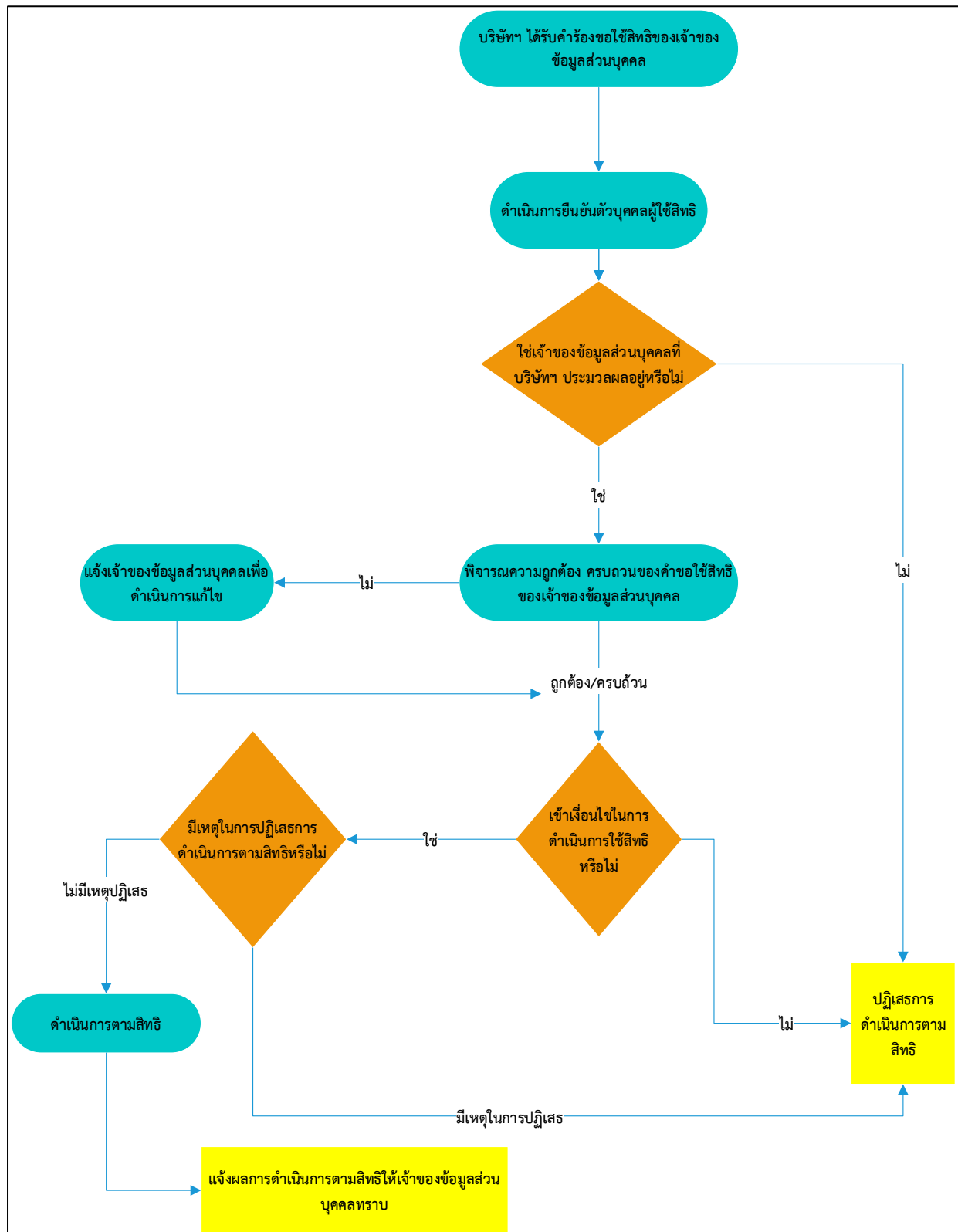
(ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมาย) ควรปฏิบัติเมื่อมีการร้องขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

ขั้นตอนการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล อาจสรุปได้ดังนี้

1. ตรวจสอบและยืนยันตัวบุคคลของผู้ยื่นคำร้องขอใช้สิทธิ (“คำร้องขอ”)
2. พิจารณาความถูกต้องของคำร้องขอ
3. พิจารณาดำเนินการตามสิทธิ
 - พิจารณาเงื่อนไขในการใช้สิทธิ
 - พิจารณาเหตุผลการใช้สิทธิ
4. แจ้งผลการพิจารณาเงื่อนไขและเหตุผล
 - แจ้งผล กรณีที่บริษัทจะดำเนินการตามสิทธิ
 - แจ้งผล กรณีที่บริษัทปฏิเสธไม่ดำเนินการตามสิทธิ
5. ดำเนินการตามสิทธิ
6. แจ้งผลการดำเนินการ เมื่อได้ดำเนินการตามสิทธิจนแล้วเสร็จ

ทั้งนี้ ขั้นตอนข้างต้นเป็นเพียงแนวทางเบื้องต้นเท่านั้น บริษัทสามารถปรับเปลี่ยนแก้ไขเพื่อให้เข้ากับแนวทางปฏิบัติภายในของบริษัทได้

ภาพรวมขั้นตอนการดำเนินการเมื่อมีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล



รายละเอียดการดำเนินการเมื่อมีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ในแต่ละขั้นตอนดังต่อไปนี้

	ขั้นตอน	คำอธิบาย
1.	ตรวจสอบและยืนยันตัวตนของผู้ยื่นคำร้องขอใช้สิทธิ	1. เมื่อมีผู้ยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลต่อ บริษัท บริษัทควรดำเนินการตรวจสอบและยืนยันตัวตนบุคคลก่อนว่า ผู้ยื่นคำร้องขอใช้สิทธิดังกล่าว เป็นเจ้าของข้อมูลส่วนบุคคลหรือไม่ หรือเป็นผู้มีอำนาจทำการแทนเจ้าของข้อมูลส่วนบุคคลหรือไม่ 2. หากคำร้องขอใช้สิทธิเป็นหนังสือ หรือผ่านช่องทางอิเล็กทรอนิกส์ (เช่น อีเมล) หรือช่องทางการติดต่อสื่อสารอื่น ๆ บริษัทควรจัดให้มีการยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลอย่างเหมาะสมก่อนดำเนินการใด ๆ ต่อ 3. กรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น บริษัทจะต้องพิจารณาต่อไปว่าบุคคลดังกล่าวมีอำนาจดำเนินการแทนเจ้าของข้อมูลส่วนบุคคลหรือไม่ (เช่น เป็นผู้ใช้อำนาจปกครอง หรือเป็นผู้รับมอบอำนาจ) ทั้งนี้ บริษัทควรจะต้องขอหลักฐานเพื่อยืนยันว่าบุคคลที่ร้องขอใช้สิทธิเป็นผู้ที่มีอำนาจในการดำเนินการดังกล่าวประกอบคำร้องขอด้วย 4. เมื่อได้ยืนยันตัวเจ้าของข้อมูลส่วนบุคคล และ/ หรือได้รับรายละเอียดที่จำเป็นตามคำร้องดังกล่าวแล้ว 4.1. พนักงานผู้รับคำร้องจะต้องดำเนินการส่งเรื่องต่อให้แก่ฝ่ายจัดการข้อมูลส่วนบุคคลของบริษัท เพื่อดำเนินการต่อไปโดยทันที หรือ 4.2. ถ้าพนักงานผู้รับคำร้องมีอำนาจหน้าที่ในการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคลอยู่แล้ว พนักงานควรดำเนินการต่อไปทันที ข้อแนะนำ • บริษัทควรเก็บรายละเอียดเกี่ยวกับการดำเนินการตามขั้นตอนนี้ไว้ เพื่อเป็นหลักฐานในกรณีมีข้อพิพาทในอนาคต

	ขั้นตอน	คำอธิบาย
		- บริษัทควรระบุช่องทางการยื่นคำร้องขอโดยเฉพาะเจาะจง เพื่อให้บริษัทสามารถบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพยากรได้อย่างเหมาะสม โดยบริษัทอาจจัดให้มีช่องทางหลักในการยื่นคำร้องขอใช้สิทธิ กล่าวคือ 1. สำนักงานใหญ่ของบริษัท (Front Counter) 2. เว็บไซต์และอีเมลของบริษัท (Website & E-mail) 3. คอลเซ็นเตอร์ของบริษัท (Call Center) ตัวอย่าง - กรณีใช้สำนักงานของบริษัทเป็นช่องทางหลักในการยื่นคำร้องขอใช้สิทธิ บริษัทอาจเตรียมแบบฟอร์มคำร้องขอใช้สิทธิ โดยมีคำถามหรือการระบุรายละเอียดเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล - กรณีใช้เว็บไซต์และอีเมลของบริษัทเป็นช่องทางหลักในการยื่นคำร้องขอใช้สิทธิ บริษัทอาจเตรียมแบบฟอร์มคำร้องขอใช้สิทธิแบบเดียวกับช่องทางสำนักงาน โดยจัดให้เจ้าของข้อมูลส่วนบุคคลสามารถกดลิงก์ (Link) ในเว็บไซต์เพื่อดาวน์โหลดแบบฟอร์มและส่งอีเมลมายังบริษัท - กรณีใช้คอลเซ็นเตอร์ของบริษัทเป็นช่องทางหลักในการยื่นคำร้องขอใช้สิทธิ บริษัทอาจเตรียมแบบฟอร์มคำร้องขอใช้สิทธิแบบเดียวกับช่องทางสำนักงาน เพื่อให้เจ้าหน้าที่คอลเซ็นเตอร์สอบถามและกรอกผู้ร้องขอ ทั้งนี้ บริษัทควรขอความยินยอมจากผู้ร้องขอเพื่อบันทึกเสียงสนทนาตลอดทั้งการสนทนา เพื่อเก็บไว้เป็นหลักฐานพร้อมกับแบบฟอร์ม
2.	พิจารณาความถูกต้องของคำร้องขอ	- บริษัทต้องพิจารณาความถูกต้องและสมบูรณ์ของคำร้องขอ โดยพิจารณาว่าเจ้าของข้อมูลส่วนบุคคลให้รายละเอียดที่จำเป็นและถูกต้องเพื่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลหรือไม่ - หากรายละเอียดที่เจ้าของข้อมูลส่วนบุคคลให้ไม่ถูกต้องหรือไม่สมบูรณ์เพียงพอที่จะดำเนินการตามสิทธิที่มีการร้องขอได้ ให้บริษัทขอข้อมูลเพิ่มเติมโดยไม่ชักช้า

	ขั้นตอน	คำอธิบาย
3.	พิจารณาดำเนินการตามสิทธิ	1. <u>พิจารณาเงื่อนไขในการใช้สิทธิ</u>: บริษัทต้องพิจารณาก่อนว่าคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามเงื่อนไขที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดหรือไม่ เนื่องจาก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีการกำหนดเงื่อนไขสำหรับการใช้สิทธิแต่ละประเภทของเจ้าของข้อมูลส่วนบุคคลไว้ต่างกัน (โปรดดูรายละเอียดในหัวข้อ 7.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล) ทั้งนี้ หากไม่เข้าเงื่อนไขก็ไม่สามารถดำเนินการตามสิทธิได้ เพราะไม่มีกฎหมายรับรองสิทธิในกรณีดังกล่าว 2. <u>พิจารณาเหตุปฏิเสธการใช้สิทธิ</u>: หากพิจารณาเงื่อนไขในการใช้สิทธิข้างต้นแล้ว บริษัทเห็นว่า เข้าเงื่อนไขในการใช้สิทธิ บริษัทจะต้องพิจารณาต่อไปว่า บริษัทมีเหตุที่สามารถปฏิเสธไม่ปฏิบัติตามสิทธิได้หรือไม่ (โปรดดูรายละเอียดในหัวข้อ 7.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล) โดยเมื่อดำเนินการตามขั้นตอนนี้เสร็จแล้ว บริษัทต้องแจ้งผลการพิจารณาต่อไป
4.	แจ้งผลการพิจารณาเงื่อนไขและเหตุปฏิเสธ	1. <u>แจ้งผล กรณีที่บริษัทจะดำเนินการตามสิทธิ</u>: บริษัทจะต้องแจ้งผลแก่ผู้ยื่นคำร้องขอให้ทราบ โดยระบุรายละเอียดในประเด็นต่าง ๆ เช่น ระยะเวลาการดำเนินการโดยประมาณ บุคคลที่รับผิดชอบ สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ เป็นต้น 2. <u>แจ้งผล กรณีที่บริษัทปฏิเสธไม่ดำเนินการตามสิทธิ</u>: บริษัทจะต้องแจ้งให้ผู้ยื่นคำร้องขอทราบถึงข้ออ้างในการปฏิเสธ จดบันทึกการปฏิเสธนั้นลงในรายการบันทึกตามหน้าที่ที่กฎหมายกำหนด⁹⁸ รวมไปถึงแจ้งสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญด้วย
5.	ดำเนินการตามสิทธิ	ดำเนินการตามคำร้องขอใช้สิทธิตามรายละเอียดที่ได้อธิบายไว้ในต่างกัน (โปรดดูรายละเอียดในหัวข้อ 7.1 สิทธิของเจ้าของข้อมูลส่วนบุคคล)

⁹⁸ มาตรา 39 (7) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

	ขั้นตอน	คำอธิบาย
		<u>หมายเหตุ</u> กรณีที่มีผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทจะต้องแจ้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ด้วย ไม่ว่าผู้ประมวลผลข้อมูลส่วนบุคคลจะอยู่ในประเทศหรือต่างประเทศก็ตาม
6.	แจ้งผลการดำเนินการตามสิทธิ	บริษัทควรจะต้องแจ้งผลการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคลแก่ผู้ยื่นคำร้องขอใช้สิทธิ โดยไม่ชักช้า นอกจากนี้ บริษัทอาจจะทำการสำรวจและประเมินผลความพึงพอใจของผู้ใช้บริการด้วย (หากมี)

หมายเหตุ

- บริษัทอาจกำหนดระยะเวลาดำเนินการในแต่ละขั้นตอนไว้เป็นการเฉพาะภายในบริษัทก็ได้ เพื่อให้แน่ใจว่าบริษัทสามารถดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ภายในระยะเวลาที่เหมาะสม
- บริษัทควรจะต้องใช้ถ้อยคำสื่อสารอย่างระมัดระวัง โดยเฉพาะในกรณีที่บริษัทจะปฏิเสธไม่ดำเนินการตามคำร้องขอใช้สิทธิ
- บริษัทควรขอให้ผู้ยื่นคำร้องขอเลือกช่องทางที่สะดวกในการติดต่อกลับไปยังผู้ยื่นคำร้องหรือเจ้าของข้อมูลส่วนบุคคลด้วย
- บริษัทควรจะต้องดำเนินการข้างต้นให้แล้วเสร็จ โดยไม่ชักช้าและไม่ควรเกิน 30 วันนับแต่ได้รับคำร้องขอ⁹⁹
- ในกรณีที่บริษัทมีการเปิดเผยข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทควรกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีขั้นตอนในรับเรื่องดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ ในสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ด้วย

7.3 แนวทางปฏิบัติเมื่อมีการร้องขอให้เปิดเผยข้อมูลส่วนบุคคลจากหน่วยงานรัฐ

เมื่อหน่วยงานรัฐหรือส่วนงานราชการใด ร้องขอให้บริษัทส่งมอบหรือให้เข้าถึงข้อมูลส่วนบุคคล บริษัทควรจัดให้มีคำถามหรือแบบสอบถามที่ตรวจสอบอำนาจหน้าที่ตามกฎหมายของทั้งหน่วยงานที่ร้องขอและเจ้าหน้าที่ผู้ร้องขอด้วยก่อนที่จะดำเนินการใด ๆ ต่อไป เพราะโดยทั่วไปแล้ว หน่วยงานรัฐหรือส่วนงานราชการ

⁹⁹ ถึงแม้ว่าจะมีเพียงพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลมาตรา 30 วรรคสี่ ที่กำหนดระยะเวลาในการดำเนินการตามคำขอใช้สิทธิเข้าถึงและรับสำเนาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล แต่บริษัทควรที่จะนำกรอบเวลานี้ มาปรับใช้เป็นกรอบเวลามาตรฐานขั้นต่ำในการดำเนินการตามคำร้องขอใช้สิทธิอื่น ๆ ของเจ้าของข้อมูลส่วนบุคคลได้ ไปพลางก่อนที่จะมีคำวินิจฉัยหรือคำแนะนำของคณะกรรมการ

ไม่อาจกระทำการใด ๆ ได้ โดยไม่มีกฎหมายให้อำนาจให้กระทำการนั้น ๆ ดังนั้น หน่วยงานรัฐหรือส่วนงานราชการจะสามารถขอข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจากบริษัทได้ เฉพาะกรณีที่มีกฎหมายให้อำนาจหน่วยงานดังกล่าวไว้

ตัวอย่าง

ศาล เช่น ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ ศาลทหาร เป็นต้น

โดยหลัก เมื่อมีคดีความขึ้นสู่ชั้นศาล ศาลจะมีอำนาจในการออกคำสั่งเรียกพยานหลักฐาน หรือหมายเรียกบุคคลให้มาเป็นพยานในกระบวนการพิจารณาคดีได้ ซึ่งพยานหรือพยานหลักฐานดังกล่าว อาจให้การหรือมีการระบุข้อมูลส่วนบุคคลก็ได้ ตามกฎหมายว่าด้วยวิธีพิจารณาคดีของศาล ตัวอย่างดังนี้

ประมวลกฎหมายวิธีพิจารณาความแพ่ง

“มาตรา 90 ให้คู่ความฝ่ายที่อ้างอิงเอกสารเป็นพยานหลักฐานเพื่อสนับสนุนข้ออ้างหรือข้อเถียงของตนตามมาตรา 88 วรรคหนึ่ง ยื่นต่อศาลและส่งให้คู่ความฝ่ายอื่นซึ่งสำเนาเอกสารนั้นก่อนวันสืบพยานไม่น้อยกว่าเจ็ดวัน

ในกรณีที่คู่ความฝ่ายใดยื่นคำแถลงหรือคำร้องขออนุญาตอ้างอิงเอกสารเป็นพยานหลักฐานตามมาตรา 88 วรรคสองหรือวรรคสาม ให้ยื่นต่อศาลและส่งให้คู่ความฝ่ายอื่นซึ่งสำเนาเอกสารนั้นพร้อมกับการยื่นคำแถลงหรือคำร้องดังกล่าว เว้นแต่ศาลจะอนุญาตให้ยื่นสำเนาเอกสารภายหลังเมื่อมีเหตุอันสมควร

คู่ความฝ่ายที่อ้างอิงพยานหลักฐานไม่ต้องยื่นสำเนาเอกสารต่อศาล และไม่ต้องส่งสำเนาเอกสารให้คู่ความฝ่ายอื่นในกรณีดังต่อไปนี้

(1) เมื่อคู่ความฝ่ายใดอ้างอิงเอกสารเป็นชุดซึ่งคู่ความฝ่ายอื่นทราบคืออยู่แล้วหรือสามารถตรวจตราให้ทราบได้โดยง่ายถึงความมีอยู่และความแท้จริงแห่งเอกสารนั้น เช่น จดหมายโต้ตอบระหว่างคู่ความในคดี หรือสมุดบัญชีการค้า และสมุดบัญชีของธนาคารหรือเอกสารในสำนวนคดีเรื่องอื่น

(2) เมื่อคู่ความฝ่ายใดอ้างอิงเอกสารฉบับเดียวหรือหลายฉบับที่อยู่ในความครอบครองของคู่ความฝ่ายอื่นหรือของบุคคลภายนอก

(3) ถ้าการคัดสำเนาเอกสารจะทำให้กระบวนการพิจารณาล่าช้าเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงเอกสารนั้น หรือมีเหตุผลแสดงว่าไม่อาจคัดสำเนาเอกสารให้เสร็จภายในกำหนดเวลาที่ให้ยื่นสำเนาเอกสารนั้น

กรณีตาม (1) หรือ(3) ให้คู่ความฝ่ายที่อ้างอิงเอกสารยื่นคำขอฝ่ายเดียวโดยทำเป็นคำร้องต่อศาล ขอ อนุญาตงดการยื่นสำเนาเอกสารนั้นและขอยื่นต้นฉบับเอกสารแทน เพื่อให้ศาลหรือคู่ความฝ่ายอื่นตรวจสอบตาม เงื่อนไขที่ศาลเห็นสมควรกำหนด

กรณีตาม (2) ให้คู่ความฝ่ายที่อ้างอิงเอกสารขอให้ศาลมีคำสั่งเรียกเอกสารนั้นมาจากผู้ครอบครองตาม มาตรา 123 โดยต้องยื่นคำร้องต่อศาลภายในกำหนดเวลาตามวรรคหนึ่งหรือวรรคสอง แล้วแต่กรณี และให้ คู่ความฝ่ายนั้นมีหน้าที่ติดตามเพื่อให้ได้เอกสารดังกล่าวมาภายในเวลาที่ศาลกำหนด”

ประมวลกฎหมายวิธีพิจารณาความอาญา

“มาตรา 239 เอกสารใดซึ่งคู่ความอ้าง แต่มิได้อยู่ในความยึดถือของเขา ถ้าคู่ความนั้นแจ้งถึงลักษณะ และที่อยู่ของเอกสารต่อศาล ให้ศาลหมายเรียกบุคคลผู้ยึดถือนำเอกสารนั้นมาส่งศาล”

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.)

สำนักงาน คปภ. โดยนายทะเบียนและพนักงานเจ้าหน้าที่ มีอำนาจในการขอข้อมูลส่วนบุคคลใด ๆ อันเกี่ยวกับการประกอบกิจการของบริษัทตามพระราชบัญญัติประกันวินาศภัย พ.ศ. 2535 มาตรา 51

พ.ร.บ. ประกันวินาศภัย พ.ศ. 2535

“มาตรา 51 ให้นายทะเบียนและพนักงานเจ้าหน้าที่มีอำนาจตรวจสอบกิจการและฐานะการเงินของ บริษัท และเพื่อประโยชน์ในการตรวจสอบให้นายทะเบียน และพนักงานเจ้าหน้าที่มีอำนาจ....

(3) สั่งให้บริษัทหรือผู้ที่เกี่ยวข้องกับธุรกิจของบริษัทส่งเอกสารหรือหลักฐานอื่น ๆ”

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

ปปง. มีอำนาจในการกำหนดให้บริษัท ซึ่งเป็นผู้ประกอบการ นำส่งข้อมูลส่วนบุคคลที่กำหนดในขั้นตอนการจัดให้ลูกค้าแสดงตนให้แก่ ปปง. ภายใต้ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน

พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน

“มาตรา 16 ให้ผู้ประกอบการอาชีพดังต่อไปนี้มีหน้าที่ต้องรายงานการทำธุรกรรมต่อสำนักงาน ในกรณีเป็นธุรกรรมที่ใช้เงินสดมีจำนวนเกินกว่าที่กำหนดในกฎกระทรวง หรือเป็นธุรกรรมที่มีเหตุอันควรสงสัย ทั้งนี้ ผู้ประกอบการอาชีพตาม (2) (3) (4) และ(5) ต้องเป็นนิติบุคคล เว้นแต่ในกรณีที่มีเหตุอันควรสงสัยที่มีพยานหลักฐานอันสมควรว่ามีการทำธุรกรรมที่เกี่ยวข้องหรืออาจเกี่ยวข้องกับการกระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินกับผู้ประกอบการอาชีพตาม (2) (3) (4) และ(5) ที่มีได้เป็นนิติบุคคล ให้สำนักงานมีอำนาจ สั่งเป็นหนังสือให้ผู้ประกอบการชีพดังกล่าวรายงานการทำธุรกรรมต่อสำนักงาน

(1) ผู้ประกอบการชีพเกี่ยวกับการดำเนินการ การให้คำแนะนำ หรือเป็นที่ปรึกษาในการทำธุรกรรมที่เกี่ยวข้องกับการ ลงทุนหรือการเคลื่อนย้ายเงินทุนตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ที่ไม่ใช่สถาบันการเงินตามมาตรา 13

(9) ผู้ประกอบการชีพเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ตามกฎหมายว่า ด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์”

กระทรวงแรงงาน

กระทรวงแรงงาน โดยพนักงานตรวจแรงงานมีอำนาจในการขอข้อมูลส่วนบุคคลใด ๆ อันอาจเกี่ยวข้องกับความปลอดภัยในการทำงาน และการกระทำการอย่างอื่นเพื่อให้ได้ข้อเท็จจริงในอันที่จะปฏิบัติการให้เป็นไปตามพระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 มาตรา 139

พ.ร.บ คุ้มครองแรงงาน พ.ศ. 2541

“มาตรา 139 ในการปฏิบัติการตามหน้าที่ ให้พนักงานตรวจแรงงานมีอำนาจ ดังต่อไปนี้

(1) เข้าไปในสถานประกอบกิจการหรือสำนักงานของนายจ้าง และสถานที่ทำงาน ของลูกจ้างในเวลาทำการ เพื่อตรวจสอบสภาพการทำงานของลูกจ้างและสภาพการจ้าง สอบถาม ข้อเท็จจริง ถ่ายภาพ ถ่ายสำเนาเอกสารที่เกี่ยวข้องกับการจ้าง การจ่ายค่าจ้าง ค่าล่วงเวลา ค่าทำงานในวันหยุด ค่าล่วงเวลาในวันหยุด และทะเบียนลูกจ้าง เก็บตัวอย่างวัสดุหรือผลิตภัณฑ์เพื่อวิเคราะห์ เกี่ยวกับความปลอดภัยในการทำงาน และกระทำการอย่างอื่นเพื่อให้ได้ข้อเท็จจริงในอันที่จะปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้”

ข้อสังเกต

- บริษัทอาจกำหนดให้มีกระบวนการยืนยันและตรวจสอบตัวตนของเจ้าพนักงานที่ร้องขอให้ส่งข้อมูลส่วนบุคคล โดยการให้ตอบคำถามในแบบฟอร์มคำร้องขอสำหรับหน่วยงานรัฐ หรือขอเอกสารหลักฐานประกอบคำร้องขอ ซึ่งอาจมีรายละเอียด เช่น ถามชื่อ-นามสกุล ขอสำเนาเลขบัตรประจำตัวเจ้าพนักงาน ชื่อองค์กร หรือหน่วยงานที่สังกัด ช่องทางการติดต่อ และรายละเอียดเกี่ยวกับผู้บังคับบัญชา เป็นต้น
- หากบริษัทเปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานรัฐ โดยที่หน่วยงานดังกล่าวไม่มีอำนาจตามกฎหมายที่จะร้องขอข้อมูลส่วนบุคคลกับบริษัท บริษัทอาจจะต้องรับผิดชอบตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- เพื่อให้เป็นแนวทางปฏิบัติที่ดี บริษัทควรจดบันทึกการร้องขอของหน่วยงานรัฐเป็นลายลักษณ์อักษร โดยมีรายละเอียดตั้งแต่เริ่มมีการติดต่อจากหน่วยงานรัฐ ไปจนถึงการดำเนินการตามคำร้องขอ หรือปฏิเสธไม่ดำเนินการ แม้กฎหมายจะไม่กำหนดก็ตาม
- หากบริษัทเห็นว่า หน่วยงานรัฐไม่มีอำนาจตามกฎหมายในการออกคำสั่งให้บริษัท ส่งข้อมูลส่วนบุคคลได้ บริษัทสามารถอุทธรณ์คำสั่งดังกล่าวได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาความศาลปกครอง

บทที่ 8 แนวทางการปฏิบัติกรณีเกิดละเมิดข้อมูลส่วนบุคคล

พ.ร.บ. คู้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล กล่าวคือกรณีที่พิจารณาแล้วว่าไม่มีความเสี่ยงดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลไม่มีหน้าที่ต้องแจ้งไปยังสำนักงาน

นอกจากนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและช้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

แนวปฏิบัติในบทที่ 8 นี้ จะนำเสนอแนวทางการปฏิบัติกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล รวมถึงการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไว้ เพื่อให้บริษัทได้มีแนวทางในการปฏิบัติให้สอดคล้องตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งมีผลบังคับใช้เมื่อวันที่ 15 ธันวาคม พ.ศ. 2565

8.1 หน้าที่และความรับผิดชอบของบริษัท กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล

ข้อพิจารณาเบื้องต้น

1) การเตรียมความพร้อมรับมือเหตุการละเมิดข้อมูลส่วนบุคคล

- บริษัทต้องระบุให้ได้ว่าเหตุการณ์ใดคือเหตุการละเมิดข้อมูลส่วนบุคคล
- บริษัทควรเข้าใจว่าเหตุการละเมิดข้อมูลส่วนบุคคลไม่ได้จำกัดอยู่เพียงความเสียหายหรือการขโมยข้อมูลส่วนบุคคล
- บริษัทควรจัดเตรียมแผนรองรับกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล
- บริษัทควรแบ่งหน้าที่ความรับผิดชอบในการบริหารจัดการเหตุการละเมิดข้อมูลส่วนบุคคลให้กับบุคคลหรือกลุ่มบุคคลภายในบริษัท
- พนักงานของบริษัทควรรู้ว่าจะขยายผลการรายงานเหตุการณ์เกี่ยวกับความปลอดภัยไปยังบุคคลหรือกลุ่มบุคคลที่เหมาะสมในบริษัท เพื่อให้พิจารณาว่าเป็นเหตุการละเมิดข้อมูลส่วนบุคคลอย่างไร

2) การตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- บริษัทควรจัดเตรียมขั้นตอนในการประเมินความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคลอันเนื่องมาจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- บริษัทควรจัดเตรียมขั้นตอนในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้แล้ว แม้ว่าจะยังไม่ทราบรายละเอียดของเหตุดังกล่าวก็ตาม
- บริษัทควรจัดเตรียมขั้นตอนในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะได้รับผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- บริษัทควรจัดเตรียมแนวทางการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไว้แล้วเบื้องต้น
- บริษัทควรเข้าใจถึงเงื่อนไขที่บริษัท ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า
- บริษัทกำหนดแนวทางในการให้ข้อมูลเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะได้รับผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพื่อให้บุคคลเหล่านี้สามารถป้องกันตนเองจากการละเมิดข้อมูลส่วนบุคคลที่อาจเกิดขึ้นเพิ่มเติมได้ ทั้งนี้ ข้อมูลข้างต้นนี้ควรรวมอยู่ในข้อความของแนวทางการเยียวยาที่บริษัทจะต้องส่งให้บุคคลเหล่านั้น
- บริษัทควรบันทึกเหตุการณ์ละเมิดไว้ทั้งหมด แม้ว่าจะไม่จำเป็นจะต้องแจ้งหรือรายงานตามกฎหมายก็ตาม

8.1.1 ความหมายของการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งออกตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดนิยามของคำว่า “การละเมิดข้อมูลส่วนบุคคล” ให้มีความหมายดังต่อไปนี้

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด”

ตัวอย่างเหตุการณ์ที่อาจถือว่าการละเมิดข้อมูลส่วนบุคคล

- การที่บุคคลที่สามเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ
- การกระทำ หรือการไม่กระทำการ โดยเจตนาหรือไม่เจตนา ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลข้อมูลส่วนบุคคล
- การส่งข้อมูลส่วนบุคคลไปยังผู้รับผิดคน
- การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- การสูญเสียความสามารถในการใช้ข้อมูลส่วนบุคคล (Ransomware)
- เกิดการเจาะระบบ (Hack) ที่บริษัทใช้งาน

8.1.2 หน้าที่แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (4) กำหนดให้เป็นหน้าที่ของบริษัท ที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่บุคคลตามกรณี ดังต่อไปนี้

ระดับของเหตุละเมิดข้อมูลส่วนบุคคล	เงื่อนไข	
	แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่มีชักช้า แต่ไม่เกิน 72 ชั่วโมงนับแต่ทราบการละเมิดข้อมูลส่วนบุคคล	แจ้งเจ้าของข้อมูลส่วนบุคคลถึงการบริการจัดการการละเมิดข้อมูลส่วนบุคคล พร้อมกับการแจ้งแนวทางการเยียวยา
การละเมิดข้อมูลส่วนบุคคลที่อาจมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✗
การละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล	✓	✓

โดยประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 ได้กำหนดไว้ว่า “เหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วยเหตุที่เกิดจาก

- การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ

- การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ภัยคุกคามทางไซเบอร์

- ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทนหรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น

โดยเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ขั้นตอนในการดำเนินงานเมื่อพบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

บริษัทควรพิจารณากำหนดแนวทางหรือวิธีการในการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ชัดเจน ทั้งนี้ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด หรือผู้ควบคุมข้อมูลส่วนบุคคล

ทราบเองว่ามีหรือน่าจะมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่าการละเมิดข้อมูลส่วนบุคคลหรือไม่

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยพิจารณา 1. มาตรการเชิงองค์กร (organizational measures) 2. มาตรการเชิงเทคนิค (technical measures) และ 3. มาตรการทางกายภาพ (physical measures) ในส่วนที่เกี่ยวข้องกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่าการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(1) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด หรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

(2) เมื่อพิจารณาจากข้อเท็จจริงแล้วเห็นว่า มีเหตุอันควรเชื่อว่าการละเมิดข้อมูลส่วนบุคคลจริง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการณ์ละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(3) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมทั้งแนวทางการเยียวยาโดยไม่ชักช้าด้วย

(4) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือ

ลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

การประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล

ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้

- (1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล
- (2) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด
- (3) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด
- (4) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่างๆ ด้วยหรือไม่ เพียงใด
- (5) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล
- (6) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- (7) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)
- (8) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคลรวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้ เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใดตามคู่มือแนวทางการประเมินความเสี่ยงและแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (เวอร์ชัน 1.0) ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ฉบับลงวันที่ 15 ธันวาคม พ.ศ. 2565

โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าวต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูลส่วน บุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
1. ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้วข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
2. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลที่ระบุตัวบุคคลได้โดยตรงรั่วไหลจากระบบคอมพิวเตอร์	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก (ความเสี่ยงสูง)

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูลส่วน บุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
ของผู้ควบคุมข้อมูลส่วน บุคคล			
3. ระบบไฟฟ้าใน call center ของผู้ควบคุม ข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบ คอมพิวเตอร์และ อุปกรณ์คอมพิวเตอร์ ของผู้ควบคุมข้อมูลส่วน บุคคลไม่สามารถ ให้บริการได้ชั่วคราว	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวไม่ อยู่ในสภาพพร้อมใช้งานเนื่องจาก ปัญหาด้านเทคโนโลยี เมื่อระบบ ไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วน บุคคลดังกล่าวก็สามารถใช้งานได้ จึง ไม่ถือว่าเป็นกรณีละเมิดข้อมูลส่วน บุคคลที่มีความเสี่ยงที่จะมีผลกระทบ ต่อสิทธิและเสรีภาพของบุคคล
4. ผู้ควบคุมข้อมูลส่วน บุคคลถูกภัยคุกคามทาง ไซเบอร์ โดยถูกโจมตี จากมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อ ควบคุมข้อมูลส่วนบุคคล ทั้งหมด และผู้ควบคุม ข้อมูลส่วนบุคคลไม่มี ข้อมูลสำรอง จึงไม่ สามารถที่จะเข้าถึงและ ใช้งานข้อมูลดังกล่าวได้	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ใน สภาพที่สามารถระบุตัวบุคคลได้ การถูกโจมตีจากมัลแวร์เรียกค่าไถ่ทำ ให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่ พร้อมใช้งาน และข้อมูลสำรองที่มีอยู่ ไม่สมบูรณ์เพียงพอที่จะให้บริการ หรือไม่สามารถเรียกใช้งานข้อมูล สำรองได้ภายในระยะเวลาที่กำหนด ของแต่ละบริษัท (ดูแผน BCP ประกอบ) นอกจากนี้ยังอาจก่อให้เกิด ความเสียหายต่อธุรกิจของผู้ควบคุม ข้อมูลส่วนบุคคล รวมถึงตัวเจ้าของ ข้อมูลส่วนบุคคล จึงต้องแจ้งเหตุ

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูลส่วน บุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
5. บริษัทได้รับการติดต่อจากลูกค้า 10 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก และทำการตรวจสอบแล้วภายใน 24 ชั่วโมงพบว่ามีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน 10 ราย	ต้องแจ้ง	ต้องแจ้งเฉพาะเจ้าของข้อมูลส่วนบุคคล 10 ราย ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ของบริษัท	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริง ในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม และอาจปรับระดับความเสี่ยงเป็นสูงได้
6. บริษัทให้บริการแบบออนไลน์ ซึ่งจำเป็นต้องมีการลงทะเบียนข้อมูลผู้ใช้บริการและกำหนดรหัสผ่าน เช่น การเรียกร้องค่าสินไหมทดแทน การตรวจสอบกรมธรรม์ประกันภัย เป็นต้น ต่อมาถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลผู้ใช้บริการและรหัสผ่านถูกเข้าถึง และถูกนำไปโพสต์บนอินเทอร์เน็ต	ต้องแจ้ง	ต้องแจ้งลูกค้าของบริษัทในส่วนที่มีข้อมูลรั่วไหลบนอินเทอร์เน็ต	เนื่องจากข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล เพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย
7. ระบบผู้ให้บริการประมวลผลข้อมูลส่วนบุคคล	ผู้ให้บริการต้องแจ้งบริษัท เพื่อให้บริษัท	บริษัทไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล	ผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริง

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูลส่วน บุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
บุคคลของบริษัทเกิด ปัญหา และไม่สามารถ แก้ไขให้กลับมาพร้อมใช้ งานภายใน Service Level Agreement ที่ กำหนด เป็นเหตุให้ ผู้ให้บริการไม่สามารถ เข้าใช้บริการได้	แจ้งสำนักงานฯ เนื่องจากมี ผลกระทบต่อกลุ่ม ลูกค้า เพราะปัญหา ดังกล่าวทำให้กลุ่ม ลูกค้าไม่สามารถ เข้าถึงข้อมูลส่วน บุคคลได้	บุคคลที่ยังไม่ได้ รับผลกระทบ เนื่องจากยังไม่เกิด ปัญหา	เพิ่มเติม หากพบว่าระบบถูกโจมตี จากภัยคุกคามทางไซเบอร์ ต้องแจ้ง บริษัทตามที่ระบุไว้ในสัญญาหรือ ข้อตกลงที่เกี่ยวข้อง บริษัทต้องแจ้ง ทั้งสำนักงานฯ และเจ้าของข้อมูลส่วน บุคคล พร้อมปรับระดับเป็นความ เสี่ยงสูง
8. บริษัทถูกภัยคุกคามทาง ไซเบอร์ โดยการโจมตี ระบบจาก Hacker ทำ ให้ประวัติข้อมูลสูญภาพ บางส่วนรั่วไหล	ต้องแจ้ง หากข้อมูล ที่รั่วไหลสามารถระบุ ตัวบุคคลได้	ต้องแจ้งเนื่องจาก ข้อมูลส่วนบุคคลที่ มีความอ่อนไหวผู้ ที่ไม่หวังดีอาจ นำไปใช้ในการ กระทำความผิด หรือมีผลกระทบ ต่อสิทธิและ เสรีภาพของ เจ้าของข้อมูลส่วน บุคคลได้	จำเป็นต้องแจ้งเหตุ หากเป็นข้อมูล ส่วนบุคคลที่มีความอ่อนไหวและ สามารถระบุ ตัวตนของผู้เอา ประกันภัยหรือบุคคลอื่นที่เกี่ยวข้อง ได้
9. บริษัทเกิดความผิดพลาด ในการส่งข้อมูลประกัน กลุ่มนักเรียนจำนวนมาก ทางอีเมลไปยังผู้ที่ไม่ เกี่ยวข้อง	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากการส่งข้อมูลดังกล่าวไม่มี การเข้ารหัส และเป็นข้อมูลส่วน บุคคลของบุคคลจำนวนมาก ซึ่งอาจมี ทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูล ส่วนบุคคลที่มีความอ่อนไหวซึ่งผู้ที่ ได้รับข้อมูลอาจจะนำข้อมูลดังกล่าว ไปใช้โดยมิชอบและก่อให้เกิดความ เสียหายได้

ตัวอย่าง	แจ้งเหตุแก่ สำนักงาน คณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่ เจ้าของข้อมูล ส่วนบุคคล	เหตุผล
10.บริษัททำการตลาดแบบตรง โดยต้องการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่เกิดความผิดพลาด จึงทำให้มีการส่งอีเมลไปยังผู้รับข้อมูลทั้งหมดจำนวน 100 คน พร้อมกัน	ต้องแจ้ง เนื่องจากมีการส่งข้อมูลส่วนบุคคลไปยังกลุ่มคนจำนวนมากที่ไม่เกี่ยวข้อง แต่หากข้อมูลดังกล่าวมีการเข้ารหัสโดยเทคโนโลยีที่น่าเชื่อถือ อาจได้รับยกเว้นไม่ต้องแจ้งเหตุ	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลหรือไม่ ขึ้นอยู่กับการเข้าถึงข้อมูล หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด จึงไม่จำเป็นต้องแจ้งเหตุ
11.บริษัทใส่อีเมลผู้รับจำนวน 100 คน เข้าไปในช่อง To หรือ CC แทนที่จะระบุไว้ในช่อง BCC ทำให้ผู้รับเห็นรายชื่ออีเมลของบุคคลอื่นที่ไม่เกี่ยวข้อง	ต้องแจ้ง เนื่องจากมีการส่งข้อมูลส่วนบุคคลไปยังกลุ่มคนจำนวนมากที่ไม่เกี่ยวข้อง	ต้องแจ้ง เนื่องจากข้อมูลส่วนบุคคลในอีเมลดังกล่าวอาจถูกนำไปใช้และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลภายหลังได้	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลหรือไม่ ขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วย

หมายเหตุ: ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลดังกล่าว เป็นเพียงแนวทางในการประเมินความเสี่ยงเท่านั้น หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณีๆ ไป

ข้อสังเกต

หากการละเมิดข้อมูลส่วนบุคคลไม่ก่อให้เกิดความเสี่ยง หรือไม่มีความเสี่ยง บริษัทไม่จำเป็นต้องแจ้งทั้งสำนักงาน และเจ้าของข้อมูลส่วนบุคคล แต่ทั้งนี้ ในทางปฏิบัติอาจเป็นการยากที่ผลของการพิจารณาความ

เสี่ยงของการละเมิดข้อมูลส่วนบุคคลนั้นเป็นกรณีที่ไม่ก่อให้เกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

8.1.3 วิธีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถทำได้

(1) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคล หรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

(3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล

(4) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลง หรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน

8.1.4 กรณีแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าเกิน 72 ชั่วโมง

ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่า 72 ชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระวังหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยเร็ว ทั้งนี้ ต้องไม่เกิน 15 วันนับแต่ทราบเหตุ

ทั้งนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง อาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกำหนดเวลาในมาตรา 37 (4) ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

อนึ่ง การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง นั้น ไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

8.1.5 ข้อยกเว้นการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง เพื่อประกอบการพิจารณาได้ หากผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าเหตุการละเมิดข้อมูลส่วนบุคคลนั้น

- ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- ข้อมูลส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

- ข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ
- เหตุอื่นใดที่เชื่อถือได้

ในการยกข้อยกเว้นดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ให้ข้อมูลหรือส่งเอกสารหรือหลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่น ๆ ที่เกี่ยวข้อง พิจารณาด้วย

8.1.6 การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำได้โดยไม่ชักช้า

- (1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
- (2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน
- (3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- (4) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อเสนอแนะเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

ในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้ เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการณ์ละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการ

ทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

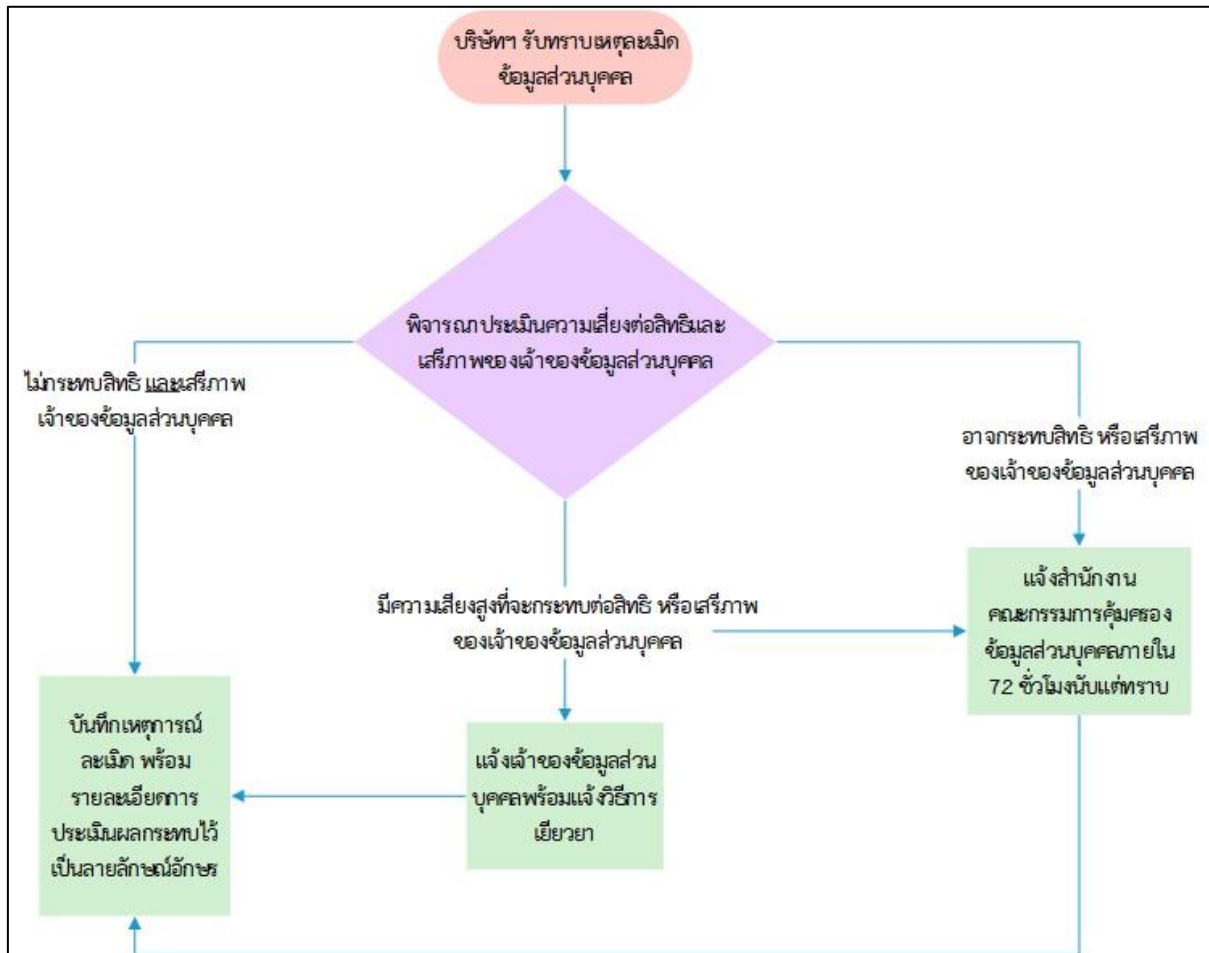
ทั้งนี้ การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

8.1.7 โทษที่เกี่ยวข้อง

หากบริษัทไม่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด บริษัทอาจถูกโทษปรับทางปกครองไม่เกิน 3 ล้านบาท ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 83 ทั้งนี้ ในกรณีที่บริษัทไม่เห็นด้วยกับการลงโทษทางปกครองข้างต้น บริษัทสามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาความของศาลปกครอง

ข้อเสนอแนะ

บริษัทควรจัดทำบันทึกเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคล การแจ้งเหตุฯ และข้อยกเว้นกรณีที่ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลที่ใช้อ้างอิงไว้ ไม่ว่าบริษัทจะได้รับยกเว้นให้ไม่ต้องแจ้งเจ้าของข้อมูลส่วนบุคคลด้วยหรือไม่ก็ตาม เพื่อเป็นหลักฐาน ในกรณีมีข้อพิพาท



8.2 กรณีศึกษาเกี่ยวกับเหตุละเมิดข้อมูลส่วนบุคคล

กรณีศึกษาที่ 1: การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Anthem, Inc. ในปีพ.ศ. 2558¹⁰⁰

ข้อเท็จจริง

ในปี พ.ศ. 2558 Anthem, Inc. ซึ่งเป็นบริษัทประกันภัยรายใหญ่ของสหรัฐอเมริกาได้ประกาศว่าข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัทได้ถูกละเมิดไปราว 3.7 ล้านชุดข้อมูล และเป็นข้อมูลส่วนบุคคลของชาวอเมริกันมากกว่า 80 ล้านคน ซึ่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวเกิดขึ้นเนื่องจากถูกแฮกเกอร์ (Hacker) นำข้อมูลส่วนบุคคลไป โดยการละเมิดข้อมูลส่วนบุคคลดังกล่าวนี้มิได้เกิดขึ้นเพียงครั้งเดียวแต่เกิดขึ้นเรื่อย ๆ ระหว่างช่วงเดือนธันวาคม พ.ศ. 2557 จนถึงเดือนกุมภาพันธ์ พ.ศ. 2558 โดยข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ อีเมล หมายเลขประกันสังคม วันเกิด หมายเลขสมาชิกประกันภัย หมายเลขผู้ป่วย ข้อมูลพนักงาน และรายได้ของบริษัท ซึ่งจากการตรวจสอบพบว่าโดยมากข้อมูลส่วนบุคคลที่ถูกละเมิดไปนั้นได้ถูกนำไปขายต่อให้กับตลาดมืด และไม่ได้มีการนำข้อมูลจำพวกประวัติสุขภาพไปใช้

นอกจากนั้นจากการตรวจสอบยังพบว่าการเกิดเหตุละเมิดนั้นอาจเป็นเพราะว่า Anthem, Inc. ไม่ได้มีระบบรักษาความปลอดภัยที่เพียงพอ กล่าวคือ Anthem, Inc. ไม่ได้มีมาตรการในการเข้ารหัสข้อมูล (Encryption) ที่มีการจัดเก็บซึ่งอาจทำให้ Hacker สามารถทำลายระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคล และเข้าถึงข้อมูลส่วนบุคคลได้โดยง่าย

บทวิเคราะห์

- จากกรณีข้างต้นทำให้เห็นว่าการจัดการเกี่ยวกับระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นเรื่องสำคัญอย่างยิ่งสำหรับผู้ควบคุมข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งผู้ควบคุมข้อมูลส่วนบุคคลที่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว ดังเช่นบริษัทประกันวินาศภัย และบริษัทประกันชีวิต เนื่องจากข้อมูลส่วนบุคคลเหล่านั้นสามารถทำให้เกิดความเสียหายหรือเกิดผลกระทบกับสิทธิและเสรีภาพของบุคคลได้ง่าย
- การเข้ารหัสข้อมูล (Encryption) เป็นวิธีหนึ่งที่จะช่วยให้บริษัทสามารถจัดการกับข้อมูลส่วนบุคคล และป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้

¹⁰⁰ <https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref> เข้าถึงเมื่อวันที่ 28 สิงหาคม พ.ศ. 2563

- ในกรณีนี้ Athem, Inc. ได้มีขั้นตอนการดำเนินการจัดการ และแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่รวดเร็ว และนำไปเป็นแบบอย่าง ตามที่เจ้าหน้าที่ FBI ได้กล่าวให้สัมภาษณ์ไว้ โดยเมื่อพนักงานของ Athem, Inc. พบข้อสงสัยเกี่ยวกับฐานข้อมูลของบริษัท บริษัทก็เริ่มดำเนินการตรวจสอบทันที และเมื่อบริษัทหาสาเหตุ และรายละเอียดเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลได้แล้ว บริษัทก็ดำเนินการแจ้ง FBI ของสหรัฐอเมริกา พร้อมทั้งส่งจดหมายแจ้งเจ้าของข้อมูลส่วนบุคคลที่อาจได้รับผลกระทบทันที โดยในการแจ้งรายละเอียดเรื่องการละเมิดข้อมูลส่วนบุคคลนั้น บริษัทได้มีการแจ้งไปถึงประเภทข้อมูลส่วนบุคคลที่ถูกขโมยไป และหลังจากนั้น Athem, Inc. ก็ได้จ้างบริษัทจัดการด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศหลายรายให้เข้าร่วมจัดการกับระบบรักษาความปลอดภัยของบริษัทเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

กรณีศึกษาที่ 2 การเกิดเหตุละเมิดข้อมูลส่วนบุคคลของ Capital One¹⁰¹

ข้อเท็จจริง

เมื่อเดือนกรกฎาคม พ.ศ. 2562 ที่ผ่านมา Capital One ซึ่งเป็นสถาบันการเงินของสหรัฐอเมริกาได้ถูกแฮกเกอร์ (Hacker) เข้าสู่ระบบฐานข้อมูลแบบ Cloud ของบริษัทโดยที่บุคคลดังกล่าวเป็นพนักงานของบริษัท Amazon Web Services (AWS) ซึ่งเป็นผู้ให้บริการด้านการจัดการข้อมูลบนระบบ Cloud ที่ Capital One ใช้บริการอยู่ โดยที่พนักงานดังกล่าวสามารถเข้าถึงข้อมูลทั้งหมดของ Capital One ได้ และได้นำเรื่องที่ตนสามารถแฮกข้อมูลของ Capital One ได้ไปโพสต์ลงในรูปของ Github ซึ่งเป็นเว็บไซต์ที่ให้บริการพื้นที่ทางอินเทอร์เน็ต สำหรับการควบคุมการปรับปรุงแก้ไขเอกสารออนไลน์โดยใช้กิต (Git)¹⁰² อันทำให้ Capital One ได้รับทราบถึงการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

ในการแฮกระบบฐานข้อมูลของ Capital One ในครั้งนี้ทำให้ข้อมูลของลูกค้าบัตรเครดิตเป็นจำนวนมากถูกขโมยไป โดยเจ้าของข้อมูลส่วนบุคคลที่ถูกขโมยไปเป็นชาวอเมริกันประมาณ 100 ล้านคน และเป็นลูกค้าชาวแคนาดาอีกประมาณ 6 ล้านคน ซึ่งข้อมูลส่วนบุคคลที่ถูกแฮกไปนั้นประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล วันเกิด หมายเลขประกันสังคม ข้อมูลที่สามารถเชื่อมโยงไปยังบัญชีธนาคาร และสถานะของบัตรเครดิตของลูกค้า

แต่อย่างไรก็ตาม จากการตรวจสอบการละเมิดข้อมูลส่วนบุคคลนี้ พบว่าข้อมูลที่ถูกแฮกไปนั้นไม่ได้ถูกนำไปใช้ หรือเผยแพร่ให้แก่บุคคลอื่นใดเลย เพียงแต่มีการไปโพสต์โดยแฮกเกอร์ว่ามีการเข้าถึงข้อมูลของ Capital One ได้เท่านั้น และนอกจากนั้นจากการตรวจสอบยังทำให้พบอีกว่าการที่พนักงานของ AWS

¹⁰¹ <https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/>, เข้าถึงเมื่อวันที่ 3 กันยายน 2563

¹⁰² Git คือ Version Control แบบ Distributed ตัวหนึ่ง เป็นระบบที่ใช้จัดเก็บและควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ชนิดใดก็ได้ ไม่ว่าจะเป็น Text File หรือ Binary File, [https://medium.com/@pakin/git-](https://medium.com/@pakin/git-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-git-is-your-friend-c609c5f8efea)

[https://medium.com/@pakin/git-](https://medium.com/@pakin/git-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-git-is-your-friend-c609c5f8efea)

สามารถเข้าถึงข้อมูลในฐานระบบของ Capital One ได้ทุกข้อมูลนั้นเป็นเพราะการใช้งาน และตั้งค่าระบบ could ที่เหมาะสม ไม่มีการตั้งค่าในเรื่องของสิทธิในการเข้าถึงข้อมูลของพนักงาน และบุคคลที่เกี่ยวข้องซึ่งโดยทั่วไปแล้วบริษัทควรจะต้องจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานเท่าที่จำเป็นตามหน้าที่ของพนักงานแต่ละคนเท่านั้น

บทวิเคราะห์

- จากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลของ Capital One ทำให้เห็นว่าการใช้ระบบ Cloud ในการจัดการข้อมูลของบริษัท ต้องใช้ความระมัดระวังอย่างยิ่งเนื่องจากการจัดการรักษาความปลอดภัยของการใช้ระบบ Cloud นั้นอาจไม่เหมือนกับการจัดการระบบรักษาความปลอดภัยของระบบที่ตั้งอยู่ในบริษัท
- การกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของพนักงานแต่ละคนให้สอดคล้องกับความจำเป็น และหน้าที่การงานเป็นสิ่งที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เนื่องจากการให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลเกินความจำเป็นอาจทำให้เกิดโอกาสสำหรับผู้เข้าถึงข้อมูลในการนำข้อมูลไปใช้โดยมิชอบได้
- การจัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลก็เป็นวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลได้วิธีหนึ่ง เนื่องจากการจัดให้มีระบบติดตาม และบันทึกการเข้าถึงข้อมูลส่วนบุคคลนี้จะทำให้บริษัทสามารถตรวจสอบได้ว่ามีบุคคลใดบ้างที่เข้าถึงข้อมูลส่วนบุคคล และบุคคลใดที่เข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งเนื่องจาก Capital One ไม่ได้จัดให้มีระบบการติดตาม หรือบันทึกการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสม เพียงพอ ทำให้ Capital One ไม่สามารถตรวจจับการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบได้เลย จนกระทั่งมีการโพสต์ในเรื่องการเข้าถึงข้อมูลของ Capital One ในกลุ่ม Github ซึ่งเป็นการโพสต์โอ้อวดความสามารถของแฮกเกอร์เอง
- บริษัทควรจัดให้มีขั้นตอนการจัดการกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เหมาะสม และตอบสนองกับเหตุการณ์อย่างทันท่วงที โดยในกรณีนี้ เมื่อ Capital One ได้รับทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแล้ว Capital One รีบดำเนินการแจ้ง FBI และเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องทันที พร้อมทั้งมีการประกาศเพื่อแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้บนเว็บไซต์ของ Capital One ด้วย โดยประกาศของ Capital One ในเรื่องการละเมิดข้อมูลส่วนบุคคลนี้สามารถเข้าดูได้ตามลิงก์นี้ <https://www.capitalone.com/facts2019/>

ข้อสังเกต

เมื่อบริษัทฯ พบหรือได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลข้างต้น การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยที่การดำเนินการตรวจสอบข้อเท็จจริงของการละเมิดข้อมูลส่วนบุคคลตามที่ระบุไว้ในกฎหมายลำดับรองนั้นจะต้องดำเนินการภายในระยะเวลา 72 ชั่วโมงด้วยเช่นกัน อย่างไรก็ตามหลักการที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR¹⁰³ มีการขยายความชัดเจนในเรื่องนี้ออกไปอีกโดยผู้ควบคุมข้อมูลส่วนบุคคลอาจใช้ช่วงระยะเวลาไม่นานในการตรวจสอบข้อเท็จจริงและทำการยืนยันว่าเหตุละเมิดข้อมูลส่วนบุคคลที่พบหรือรับแจ้งนั้นได้เกิดขึ้นจริงหรือไม่ และภายในช่วงระยะเวลานั้นยังถือไม่ได้ว่าบริษัทฯ ได้ ‘รับทราบ’ การละเมิดข้อมูลส่วนบุคคลแล้ว

“After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation, the controller may not be regarded as being “aware”.”

ดังนั้น จากการพิจารณาการตีความ GDPR ดังกล่าว บริษัทฯ ย่อมสามารถจัดให้มีระบบงานหรือขั้นตอนภายในซึ่งมีกระบวนการที่ใช้ระยะเวลาไม่นานนัก โดยคำนึงถึงโครงสร้างองค์กรของตนเพื่อการตรวจสอบยืนยันการเกิดเหตุตามข้อเท็จจริงดังกล่าว และช่วงเวลานั้นบริษัทฯ ยังไม่สามารถพิจารณาได้ว่าได้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเพื่อเริ่มนับกำหนดระยะเวลา 72 ชั่วโมงที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ และหน่วยงานรัฐที่เกี่ยวข้อง

¹⁰³ Guidelines 9/2022 on personal data breach notification under GDPR

บทที่ 9 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

9.1 หน้าที่ในการตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ทั้งผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้แทนของบุคคลทั้งสองดังกล่าว (กรณีผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกประเทศไทยและต้องตั้งตัวแทน (Local Representative) ในประเทศไทย) มีหน้าที่จะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลมีการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

9.1.1 ลักษณะของบุคคลที่มีหน้าที่ต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ จะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

1.1 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานรัฐตามที่คณะกรรมการประกาศกำหนด

1.2 การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคลนั้นจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

1.3 กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ข้อสังเกต

- สำหรับบริษัทนั้นอาจเข้าหลักเกณฑ์ที่ต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ 2 กรณี กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจำนวนมาก และการที่กิจกรรมหลักของบริษัท เป็นการประมวลผลข้อมูลสุขภาพ
- ในกรณีที่แม้บริษัทไม่เข้าหลักเกณฑ์ในการตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย แต่ย่อมเป็นการดีสำหรับบริษัทที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมาช่วยทำหน้าที่ในการกำกับดูแล ให้คำปรึกษาเกี่ยวกับการดำเนินการของบริษัท ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

9.1.2 การตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทในเครือหรือในกลุ่ม

ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันอาจตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมกันได้ โดยมีเงื่อนไขดังนี้

1) เป็นบริษัทในเครือกิจการหรือเครือธุรกิจเดียวกัน ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด (หลักเกณฑ์เดียวกับหลักเกณฑ์พิจารณาเครือกิจการหรือเครือธุรกิจในเรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ตามมาตรา 29)

2) สถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในเครือธุรกิจหรือเครือกิจการต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

9.2 คุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ปัจจุบัน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยังไม่ได้มีการกำหนดลักษณะหรือคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน แต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้ให้อำนาจคณะกรรมการในการออกประกาศเพื่อกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เมื่อพิจารณาจากหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแล้ว บริษัทอาจพิจารณากำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้

1. คุณสมบัติด้านความรู้ความเข้าใจใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

เนื่องจากหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ การให้คำแนะนำ และตรวจสอบการดำเนินการให้บริษัท ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมตลอดถึงการประสานงานกับหน่วยงานของรัฐที่เกี่ยวข้อง ดังนั้น คุณสมบัติแรกและคุณสมบัติหลักที่บริษัทควรคำนึงถึงเมื่อจะตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือ ความรู้ความเข้าใจเกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

2. คุณสมบัติทางด้านการประสบการณ์และความเข้าใจในธุรกิจประกันภัย

นอกจากความรู้ความเข้าใจใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แล้ว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรมีความเข้าใจในลักษณะการประกอบธุรกิจประกันภัยอันเป็นธุรกิจของบริษัทด้วย เนื่องจากหนึ่งในหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคือ หน้าที่ในการให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่ผู้ควบคุมข้อมูลส่วนบุคคล (บริษัท) รวมถึงพนักงาน ลูกจ้าง หรือผู้รับจ้างของบริษัท ดังนั้น การที่เจ้าของข้อมูลส่วนบุคคลเข้าใจในลักษณะของธุรกิจประกันภัยของบริษัท จะทำให้การให้คำแนะนำในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เหมาะสมกับการประกอบธุรกิจของบริษัท

3. คุณสมบัติส่วนบุคคลอื่น ๆ

เนื่องจากหนึ่งในหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ การประสานงาน ให้ความร่วมมือกับสำนักงาน พนักงาน/ลูกจ้าง ผู้รับจ้าง และเจ้าของข้อมูลส่วนบุคคล ดังนั้นบริษัทอาจพิจารณาถึงคุณสมบัติอื่น ๆ ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เช่น

- **ทักษะการด้านการสื่อสาร** – โดยเฉพาะอย่างยิ่งด้านภาษา เนื่องจากเจ้าของข้อมูลส่วนบุคคลจะต้องประสานงานกับบุคคลต่าง ๆ รวมถึงหน่วยงานของรัฐ การสื่อสารที่ดี เช่น การพูด การอธิบาย รวมถึงความคล่องแคล่วในการใช้ภาษาไทย (และภาษาอังกฤษ) จึงเป็นคุณสมบัติหนึ่งที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรมี
- **ทักษะด้านการแก้ไขปัญหา** – เนื่องจากบริษัทจะต้องแจ้งรายละเอียดในการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล (ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) ดังนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท อาจต้องรับมือกับคำถาม ข้อสงสัย หรือการร้องเรียนจากเจ้าของข้อมูลส่วนบุคคล
- **ทักษะด้านการทำงานร่วมกับผู้อื่น** – ตามที่ได้กล่าวข้างต้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจต้องประสานงานกับบุคคลอื่น รวมทั้งหน่วยงานของรัฐ
- **ความสามารถหรือความเชี่ยวชาญในทางด้านวิชาชีพอื่น ๆ** เช่น มีความรู้ความเข้าใจในกฎหมายหรือกฎเกณฑ์ของธุรกิจประกันภัย ความรู้ด้านเทคโนโลยีสารสนเทศ ความรู้ด้านการบริหารจัดการ หรืออื่น ๆ ตามแต่ความต้องการของบริษัท

9.3 เงื่อนไขเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดเงื่อนไข หรือลักษณะของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้บางประการ ดังนี้

1) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็นผู้รับจ้างบริการตามสัญญาก็ได้

จากลักษณะดังกล่าวข้างต้น สามารถพิจารณาได้ว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถตั้งขึ้นได้หลายลักษณะ ดังต่อไปนี้

พนักงานของผู้ควบคุมข้อมูลส่วนบุคคล

บริษัทอาจเลือกที่จะแต่งตั้งพนักงานของบริษัท เพื่อให้รับหน้าที่ หรือดำรงตำแหน่งเป็นเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคลของบริษัท ซึ่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจมีมากกว่า 1 คนก็ได้

ทั้งนี้ บริษัทอาจตั้งคณะทำงานที่เกี่ยวข้องกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อสนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งคณะทำงานอาจประกอบด้วยบุคคลจากแผนกต่าง ๆ ของบริษัทได้ โดยอาจกำหนดแนวทางการดำเนินงานของคณะทำงานขึ้น เพื่อเป็นแนวทางในการดำเนินงานต่าง ๆ แบ่งหน้าที่รับผิดชอบ รวมถึงอาจมีการกำหนดอำนาจในการตัดสินใจในแต่ละเรื่อง

บุคคลภายนอกผู้ให้บริการ

เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีเพียงการกำหนดว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สามารถเป็นได้ทั้งพนักงานของบริษัท หรือผู้ให้บริการตามสัญญา โดยมิได้มีการกำหนดห้ามมิให้ผู้รับจ้าง ให้บริการเป็นนิติบุคคล ประกอบกับทางปฏิบัติทั่วไปของต่างประเทศ มีการให้บริการการดำเนินการเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท (DPO Service) กันอย่างแพร่หลาย ซึ่งหากผู้ให้บริการดังกล่าว มีคุณสมบัติครบถ้วนตามที่บริษัทต้องการและตามที่คณะกรรมการอาจกำหนด บริษัทก็อาจพิจารณาตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้ให้บริการซึ่งเป็นบุคคลภายนอกได้

2) ข้อจำกัดในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตามมาตรา 42 วรรคท้าย กำหนดว่า “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้”

ดังนั้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทอาจปฏิบัติหน้าที่อื่นที่ได้รับมอบหมายได้ โดยมีเงื่อนไขว่า หน้าที่อื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องไม่ขัดหรือแย้งกับหน้าที่ในการปฏิบัติงานในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตามแนวทางปฏิบัติของต่างประเทศ ปัจจัยในการพิจารณาว่าหน้าที่อื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขัดหรือแย้งกับหน้าที่ความเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ

- 1) หน้าที่อื่นต้องไม่เกี่ยวข้องกับการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- 2) หน้าที่อื่นต้องไม่ทำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลคำนึงถึงผลประโยชน์หรือหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลน้อยลง เช่น หากหน้าที่อื่นทำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องเลือก

ผลประโยชน์ทางธุรกิจเป็นลำดับแรก และการปฏิบัติหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นลำดับรอง หน้าที่นั้นเป็นอันขัดหรือแย้งกับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่าง

- **หน้าที่ที่ไม่ขัดหรือแย้งกับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** – บริษัทกำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้ดูแล ควบคุมการบันทึกการประมวลผลข้อมูลส่วนบุคคล ตามมาตรา 39
- **หน้าที่ที่ขัดหรือแย้งกับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** – เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำรงตำแหน่งหัวหน้าฝ่ายการตลาด ซึ่งมีอำนาจตัดสินใจในการกำหนดลักษณะของกิจกรรมทางการตลาด รวมถึงกำหนดกลุ่มลูกค้าเป้าหมาย และกำหนดประเภทข้อมูลส่วนบุคคลที่จะใช้ในการดำเนินการทางการตลาดในแต่ละโครงการ เช่นนี้ หน้าที่อื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพิจารณาได้ว่าขัดหรือแย้งกับหน้าที่ในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เนื่องจากหากในฐานะหัวหน้าฝ่ายการตลาดย่อมคำนึงถึงผลจากการดำเนินการทางการตลาดเป็นหลัก รวมถึงคำนึงถึงการได้มาซึ่งข้อมูลส่วนบุคคลของลูกค้าหรือกลุ่มลูกค้าเป้าหมาย โดยอาจทำให้คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลน้อยลงได้

9.4 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้กำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ ดังนี้

- 1) ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าว
- 2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าว เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- 3) ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าวในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- 4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

นอกจากนั้นเนื่องจากมาตรา 23 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียด และช่องทางการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ อีกทั้ง มาตรา 41 วรรค 5 ยังกำหนดว่า “ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานทราบ ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ได้” ดังนั้น จึงอาจพิจารณาได้ว่า เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็มีหน้าที่ในการเป็นผู้ติดต่อหลัก (Contact Person) ในการสื่อสารกับเจ้าของข้อมูลส่วนบุคคลในเรื่องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และการปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย

9.5 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

นอกจากหน้าที่ในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลยังมีหน้าที่อื่น ๆ ที่เกี่ยวข้องดังต่อไปนี้

1) แจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้สำนักงานและเจ้าของข้อมูลส่วนบุคคลทราบ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

2) สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจัดหาเครื่องมือหรืออุปกรณ์ที่เพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

3) ห้ามให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้าง เพราะเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

4) ต้องทำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถรายงานเกี่ยวกับปัญหาในการปฏิบัติหน้าที่ไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้โดยตรง

9.6 การกระทำความผิดที่อาจเกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ไม่ได้กำหนดโทษ หรือความรับผิดไว้สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้ในบางกรณี เช่น กรณีที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นจากการปฏิบัติหน้าที่ในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและนำข้อมูลเหล่านั้นไปเปิดเผยแก่บุคคลอื่น

“มาตรา 80 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

- 1) การเปิดเผยตามหน้าที่
- 2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี
- 3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- 4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- 5) การเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ”

บทที่ 10 ความรับผิดและบทกำหนดโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

10.1 สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
1.	หลักการคุ้มครองข้อมูลส่วนบุคคล ไม่ได้เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล	มาตรา 83 มาตรา 22	★	ปรับไม่เกิน 3,000,000 บาท	✖
2.	เงื่อนไขการแจ้ง ไม่แจ้งรายละเอียดตามรายการที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 23 กำหนด แก่เจ้าของข้อมูลส่วนบุคคล	มาตรา 82 มาตรา 23	★	ปรับไม่เกิน 1,000,000 บาท	✖
3.	เงื่อนไขการแจ้ง เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น และไม่ได้แจ้งรายละเอียดตามมาตรา 23 ให้เจ้าของข้อมูลส่วนบุคคลทราบ (กรณีที่ต้องขอความยินยอม)	มาตรา 82 มาตรา 23 มาตรา 25 วรรค 2	★	ปรับไม่เกิน 1,000,000 บาท	✖
4.	เงื่อนไขความยินยอม ไม่ได้ขอความยินยอมตามแบบที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	มาตรา 82 มาตรา 19 วรรค 3	★	ปรับไม่เกิน 1,000,000 บาท	✖
5.	เงื่อนไขความยินยอม ขอความยินยอมจากเจ้าของข้อมูลโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคล	มาตรา 83	★	ปรับไม่เกิน 3,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
6.	การถอนความยินยอม ไม่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลถึงผลกระทบของการเพิกถอนความยินยอม	มาตรา 82 มาตรา 19 วรรค 6	★	ปรับไม่เกิน 1,000,000 บาท	✖
7.	วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ไม่ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือขณะที่เก็บรวบรวม	มาตรา 83 มาตรา 21	★	ปรับไม่เกิน 3,000,000 บาท	✖
8.	วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล กรณีรับข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลอื่น และใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคล (ผู้ส่ง) ในการขอรับข้อมูลส่วนบุคคลนั้น	มาตรา 83 มาตรา 27 วรรค 2	★	ปรับไม่เกิน 3,000,000 บาท	✖
9.	วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นแต่ไม่ได้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ (กรณีต้องแจ้งและขอความยินยอม)	มาตรา 83 มาตรา 21 มาตรา 25	★	ปรับไม่เกิน 3,000,000 บาท	✖
10.	การประมวลผลข้อมูลส่วนบุคคล เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่มีฐานตามกฎหมายตามมาตรา 24	มาตรา 83 มาตรา 24	★	ปรับไม่เกิน 3,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	- ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ - ไม่มีฐานโดยชอบด้วยกฎหมายอื่นในการประมวลผล				
11.	การประมวลผลข้อมูลส่วนบุคคล เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรงโดยไม่เข้ากรณียกเว้นดังนี้ 1. แจ้ง + ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนด 2. เก็บรวบรวมข้อมูลส่วนบุคคลตามข้อยกเว้นในมาตรา 24 หรือมาตรา 26	มาตรา 83 มาตรา 25 วรรค 1	★	ปรับไม่เกิน 3,000,000 บาท	✖
12.	การประมวลผลข้อมูลส่วนบุคคล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยโดยไม่มีฐานตามกฎหมายตามมาตรา 24 - ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ - ไม่มีฐานโดยชอบด้วยกฎหมายอื่นในการประมวลผล	มาตรา 83 มาตรา 27 วรรค 1	★	ปรับไม่เกิน 3,000,000 บาท	✖
13.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 41 วรรค 1 กำหนด	มาตรา 82 และ มาตรา 41 วรรค 1	★	ปรับไม่เกิน 1,000,000 บาท	✖
14.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดหาเครื่องมือหรืออุปกรณ์ที่เพียงพอและให้การช่วยเหลือ เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นสามารถปฏิบัติ	มาตรา 82 และ มาตรา 42 วรรค 2	★	ปรับไม่เกิน 1,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	ตามหน้าที่ได้หรืออำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล				
15.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เลิกจ้างพนักงานของตนด้วยเหตุที่พนักงานรายนั้นปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา 82 และ มาตรา 42 วรรค 3	★	ปรับไม่เกิน 1,000,000 บาท	✖
16.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถรายงานปัญหาในการปฏิบัติงานไปยังผู้บริหารสูงสุดได้	มาตรา 82 และ มาตรา 42 วรรค 3	★	ปรับไม่เกิน 1,000,000 บาท	✖
17.	การโอนข้อมูลไปต่างประเทศ ไม่ได้ปฏิบัติตามหลักเกณฑ์เรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ - โอนข้อมูลส่วนบุคคลไปยังประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ - ไม่เข้าข้อยกเว้นอื่นใด	มาตรา 83 มาตรา 28	★	ปรับไม่เกิน 3,000,000 บาท	✖
18.	การโอนข้อมูลไปต่างประเทศ โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศโดยไม่ปฏิบัติตาม Blinding Corporate Rules ที่ได้รับการรับรองแล้ว	มาตรา 83 มาตรา 29	★	ปรับไม่เกิน 3,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
19.	การโอนข้อมูลไปต่างประเทศ กรณีที่ยังไม่มีการกำหนดมาตรฐานความคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 28 หรือยังไม่มี BCR โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ต่างประเทศโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยไม่ได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และไม่มีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด	มาตรา 83 มาตรา 29	★	ปรับไม่เกิน 3,000,000 บาท	✖
20.	สิทธิของเจ้าของข้อมูลส่วนบุคคล ไม่ดำเนินการตามคำขอเข้าถึงข้อมูลส่วนบุคคล หรือขอรับสำเนาข้อมูลส่วนบุคคล หรือดำเนินการตามคำขอเกิน 30 วันนับแต่วันที่ได้รับคำขอ	มาตรา 82 มาตรา 30 วรรค 4	★	ปรับไม่เกิน 1,000,000 บาท	✖
21.	สิทธิของเจ้าของข้อมูลส่วนบุคคล เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แม้ว่าเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านถูกต้อง	มาตรา 83 มาตรา 32 วรรค 2	★	ปรับไม่เกิน 3,000,000 บาท	✖
22.	หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล โดยเป็นการฝ่าฝืน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	มาตรา 83 มาตรา 37	★	ปรับไม่เกิน 3,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
23.	หน้าที่การบันทึก ไม่จัดให้มีบันทึกการประมวลผลตามรายการตามที่กำหนดในมาตรา 39 วรรค 1	มาตรา 82 มาตรา 39 วรรค 1	★	ปรับไม่เกิน 1,000,000 บาท	✖
ความผิดเกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว					
24.	เงื่อนไขความยินยอม/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยปราศจากความยินยอมของเจ้าของข้อมูลโดยชัดแจ้ง	มาตรา 84 มาตรา 26 วรรค 1	★	ปรับไม่เกิน 5,000,000 บาท	✖
25.	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมโดยไม่อยู่ภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือไม่ได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด	มาตรา 84 มาตรา 26 วรรค 2	★	ปรับไม่เกิน 5,000,000 บาท	✖
26.	เงื่อนไขความยินยอม/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยไม่มีฐานตามกฎหมายตามมาตรา 26 - ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ - ไม่มีฐานโดยชอบด้วยกฎหมายอื่นในการประมวลผล	มาตรา 84 มาตรา 26 มาตรา 27 วรรค 1	★	ปรับไม่เกิน 5,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	+ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	มาตรา 79			จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ (ยอมความได้)
	และ/ หรือ	และ			
	+ โดยมีวัตถุประสงค์เพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น	มาตรา 26 มาตรา 27 วรรค 1			จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ (ยอมความได้)
27.	วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว กรณีรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวจากผู้ควบคุมข้อมูลส่วนบุคคลอื่น และใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคล (ผู้ส่ง) ในการขอรับข้อมูลส่วนบุคคลนั้น	มาตรา 84 มาตรา 26 มาตรา 27 วรรค 2	★	ปรับไม่เกิน 5,000,000 บาท	✕
	+ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	มาตรา 79 และ			จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
		มาตรา 26 มาตรา 27 วรรค 2			(ยอมความได้)
	และ/ หรือ				
	+ โดยมีวัตถุประสงค์เพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น				จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ (ยอมความได้)
28.	การโอนข้อมูลไปต่างประเทศ/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว โอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังต่างประเทศโดยที่ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและไม่เข้ากรณียกเว้นอื่นตามที่กำหนดในมาตรา 28	มาตรา 84 มาตรา 26 มาตรา 28	★	ปรับไม่เกิน 5,000,000 บาท	✖
	+ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	มาตรา 79 และ มาตรา 26 มาตรา 28	★		จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ (ยอมความได้)
	และ/ หรือ				

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	+ โดยมีวัตถุประสงค์เพื่อแสวงหาประโยชน์ที่มีควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น				จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ (ยอมความได้)
29.	การโอนข้อมูลไปต่างประเทศ/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว โอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศโดยไม่ปฏิบัติตาม Blinding Corporate Rules ที่ได้รับการรับรองแล้ว	มาตรา 84 มาตรา 26 มาตรา 29 วรรค 1	★	ปรับไม่เกิน 5,000,000 บาท	✖
30.	การโอนข้อมูลไปต่างประเทศ/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว กรณีที่ยังไม่มีการกำหนดมาตรฐานความคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 28 หรือยังไม่มี BCR โอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ต่างประเทศโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยไม่ได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และไม่มีมาตรการเยียวยาทางกฎหมายที่มี	มาตรา 84 มาตรา 26 มาตรา 29 วรรค 3	★	ปรับไม่เกิน 5,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	ประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด				
ความผิดสำหรับบุคคลที่เกี่ยวข้อง					
31.	หน้าที่การบันทึก ไม่จัดบันทึกรายการ ตามที่กำหนดไว้ในมาตรา 39 สำหรับ ตัวแทน	มาตรา 88 มาตรา 39 วรรค 1 และ 2	★	ปรับไม่เกิน 1,000,000 บาท	✖
32.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สำหรับ ตัวแทน	มาตรา 88 มาตรา 41	★	ปรับไม่เกิน 1,000,000 บาท	✖
33.	ไม่ปฏิบัติตามคำสั่งให้ส่งเอกสารหรือข้อมูลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ ของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง (รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)	มาตรา 89 มาตรา 75	✖	ปรับไม่เกิน 500,000 บาท	✖
34.	ไม่มาให้ข้อมูล หรือไม่ส่งเอกสารหรือหลักฐาน เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่	มาตรา 89 มาตรา 76 (1)	✖	ปรับไม่เกิน 500,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	(รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)				
35.	ไม่อำนวยความสะดวกตามสมควรแก่พนักงานเจ้าหน้าที่ ในการปฏิบัติหน้าที่ (รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)	มาตรา 89 มาตรา 76 วรรค 4	✖	ปรับไม่เกิน 500,000 บาท	✖
36.	ความรับผิดของกรรมการ กรณีที่ผู้กระทำความผิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือบุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคลนั้น มีหน้าที่ในการสั่งการ หรือกระทำการแต่ละเว้นไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด	มาตรา 81	✖	✖	รับโทษอาญาตามที่บัญญัติไว้เป็นความผิดนั้น ๆ
37.	ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และนำไปเปิดเผยแก่ผู้อื่น (สำหรับบุคคลใด ๆ ที่เกี่ยวข้องกับการดำเนินการของบริษัท เช่น DPO หรือกรรมการ)	มาตรา 80	✖	✖	จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

10.2 ความรับผิดและการกระทำความผิดของผู้ประมวลผลข้อมูลส่วนบุคคล

สรุปความรับผิดและบทกำหนดโทษของผู้ประมวลผลข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
1.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 41 วรรค 1 กำหนด	มาตรา 85 และ มาตรา 41 วรรค 1	★	ปรับไม่เกิน 1,000,000 บาท	✖
2.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดหาเครื่องมือหรืออุปกรณ์ที่เพียงพอ และให้การช่วยเหลือ เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นสามารถปฏิบัติตามหน้าที่ได้หรืออำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา 85 และ มาตรา 42 วรรค 2	★	ปรับไม่เกิน 1,000,000 บาท	✖
3.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เลิกจ้างพนักงานของตนด้วยเหตุที่พนักงานรายนั้นปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา 85 และ มาตรา 42 วรรค 3	★	ปรับไม่เกิน 1,000,000 บาท	✖
4.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถรายงานปัญหาในการปฏิบัติงานไปยังผู้บริหารสูงสุดได้	มาตรา 85 และ มาตรา 42 วรรค 3	★	ปรับไม่เกิน 1,000,000 บาท	✖
5.	หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยปราศจากเหตุผลที่สมควร	มาตรา 86 มาตรา 40	★	ปรับไม่เกิน 3,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ประมวลผลข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
6.	การตั้งตัวแทน ไม่แต่งตั้งตัวแทนในประเทศไทย กรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกประเทศและตกอยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 38	มาตรา 86 มาตรา 37(5) มาตรา 38	★	ปรับไม่เกิน 3,000,000 บาท	✖
7.	การโอนข้อมูลไปต่างประเทศ โอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศโดยไม่ปฏิบัติตาม Blinding Corporate Rules ที่ได้รับการรับรองแล้ว	มาตรา 86 มาตรา 29 วรรค 1 หรือ 3	★	ปรับไม่เกิน 3,000,000 บาท	✖
8.	การโอนข้อมูลไปต่างประเทศ/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว โอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันที่เป็นการขัดต่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	มาตรา 87 มาตรา 26 มาตรา 29 วรรค 1	★	ปรับไม่เกิน 5,000,000 บาท	✖
9.	การโอนข้อมูลไปต่างประเทศ/ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว กรณีที่ยังไม่มีกำหนดมาตรฐานความคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 28 หรือยังไม่มี BCR โอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังผู้ควบคุมข้อมูลส่วนบุคคล	มาตรา 87 มาตรา 26 มาตรา 29 วรรค 3	★	ปรับไม่เกิน 5,000,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ประมวลผลข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	บุคคลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ต่างประเทศโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยไม่ได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และไม่มีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด				
ความผิดสำหรับบุคคลที่เกี่ยวข้อง					
10.	หน้าที่การบันทึก ไม่จดบันทึกรายการ ตามที่กำหนดไว้ในมาตรา 39 สำหรับ ตัวแทน	มาตรา 88 มาตรา 39 วรรค 1 และ 2	★	ปรับไม่เกิน 1,000,000 บาท	✖
11.	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สำหรับ ตัวแทน	มาตรา 88 มาตรา 41	★	ปรับไม่เกิน 1,000,000 บาท	✖
12.	ไม่ปฏิบัติตามคำสั่งให้ส่งเอกสารหรือข้อมูลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ ของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง	มาตรา 89 มาตรา 75	✖	ปรับไม่เกิน 500,000 บาท	✖

สรุปความรับผิดและบทกำหนดโทษของผู้ประมวลผลข้อมูลส่วนบุคคล					
	ลักษณะการกระทำความผิด	บทบัญญัติที่เกี่ยวข้อง	ความรับผิด/โทษ		
			ความรับผิดทางแพ่ง	โทษทางปกครอง	โทษอาญา
	(รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)				
13.	ไม่มาให้ข้อมูล หรือไม่ส่งเอกสารหรือหลักฐาน เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล นี้ ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ (รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)	มาตรา 89 มาตรา 76 (1)	✖	ปรับไม่เกิน 500,000 บาท	✖
14.	ไม่อำนวยความสะดวกตามสมควรแก่พนักงานเจ้าหน้าที่ ในการปฏิบัติหน้าที่ (รวมไปถึง ตัวแทน DPO หรือบุคคลใด ๆ ก็ตาม)	มาตรา 89 มาตรา 76 วรรค 4	✖	ปรับไม่เกิน 500,000 บาท	✖
15.	ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ่มครองข้อมูลส่วนบุคคล และนำไปเปิดเผยแก่ผู้อื่น (สำหรับบุคคลใด ๆ ที่เกี่ยวข้องกับการดำเนินการของบริษัท เช่น DPO หรือกรรมการ)	มาตรา 80	✖	✖	จำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

หมายเหตุ

- ★ หมายถึง กรณีที่อาจมีโอกาสดังกล่าวเกิดขึ้นได้ โดยการใช้ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนหรือไม่ต้องพิจารณาข้อเท็จจริงเป็นรายกรณีไป กล่าวคือ การกระทำความผิดนั้น ๆ เกิดความเสียหายและสามารถพิสูจน์ความเสียหายได้หรือไม่
- เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเกี่ยวกับการฝ่าฝืนการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล รวมถึงการไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ โดยคำสั่งของคณะกรรมการผู้เชี่ยวชาญ มีฐานะเป็นคำสั่งทางปกครอง
- โทษทางปกครองนั้น มีฐานะเป็นคำสั่งทางปกครอง ผู้ถูกลงโทษสามารถอุทธรณ์โต้แย้งคำสั่งทางปกครองได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง และกฎหมายว่าด้วยจัดตั้งศาลปกครองและวิธีพิจารณาคดีปกครอง ตามลำดับ

ข้อสังเกต

การกระทำความผิดของผู้ประมวลผลข้อมูลส่วนบุคคลไม่มีโทษทางอาญา เว้นแต่โทษเกี่ยวกับการเปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ตามมาตรา 80 ซึ่งเป็นการกระทำความผิดเฉพาะบุคคล

10.3 รายละเอียดความรับผิดทางแพ่ง

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้กำหนด ความรับผิดทางแพ่งไว้ในมาตรา 77 เป็นพิเศษแตกต่างไปจากหลักกฎหมายละเมิดทั่วไปตาม ป.พ.พ. ดังนั้นในส่วนนี้จึงจะอธิบายรายละเอียด เช่น องค์ประกอบ ข้อยกเว้น ผลของการฝ่าฝืนหรือไม่ปฏิบัติตาม และอายุความของมาตราดังกล่าว ดังนี้

องค์ประกอบของความรับผิดทางแพ่งตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 77

- 1) ผู้กระทำความผิดมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล
- 2) บุคคลดังกล่าวดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืน หรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- 3) การดำเนินการอันฝ่าฝืน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล

ข้อสังเกต

ข้อแตกต่างของความรับผิดทางแพ่งตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 77 กับหลักกฎหมายละเมิดทั่วไปตาม ป.พ.พ. คือ ความรับผิดทางแพ่งข้างต้น ไม่จำเป็นต้องพิสูจน์ว่าการกระทำฝ่าฝืน หรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่

ข้อยกเว้นความรับผิด

- 1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย
- 2) ความเสียหายเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง
- 3) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ตัวอย่าง

เจ้าพนักงานควบคุมโรคติดต่อ มีหนังสือให้บริษัทเปิดเผยข้อมูลส่วนบุคคลของผู้เอาประกันภัย อุบัติเหตุการเดินทาง ที่เดินทางไปและกลับจากประเทศที่เป็นกลุ่มเสี่ยงโรคติดต่ออันตราย เพื่อใช้ประกอบการควบคุมโรคติดต่ออันตราย ตามพระราชบัญญัติโรคติดต่อ พ.ศ. 2558 กรณีนี้แม้ว่าบริษัทจะไม่ได้ปฏิบัติตามหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด บริษัทก็ได้รับยกเว้นความรับผิดทางแพ่ง

ผลของการฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

เมื่อผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จะต้องรับผิดชอบทางแพ่งและต้องชำระค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล

ทั้งนี้ ค่าสินไหมทดแทน หมายความว่ารวมถึง ค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไป ตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

นอกจากนี้ ค่าสินไหมทดแทนข้างต้น ที่เป็นค่าสินไหมทดแทนที่แท้จริงแล้ว ศาลยังมีอำนาจกำหนดค่าสินไหมทดแทนเพื่อการลงโทษ¹⁰⁴ ตามที่ศาลเห็นสมควรด้วย แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง โดยในการกำหนดค่าสินไหมทดแทนเชิงการลงโทษนั้น ศาลจะคำนึงถึงพฤติการณ์ต่าง ๆ เช่น

- ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ
- ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ
- สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น
- การที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

ข้อสังเกต

ค่าสินไหมทดแทนสำหรับความรับผิดทางแพ่งภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล นี้ อาจจะมีปัญหาในทางปฏิบัติเกี่ยวกับการคำนวณค่าสินไหมทดแทน เพราะหากความเสียหายที่เกิดขึ้น เกิดแต่เพียงความเสียหายจากการละเมิดสิทธิความเป็นส่วนตัว แต่ไม่ได้เกิดความเสียหายต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล จะเป็นการยากที่จะคำนวณค่าสินไหมทดแทนเป็นตัวเงิน

อายุความฟ้องเรียกค่าสินไหมทดแทน¹⁰⁵

สิทธิค่าเสียหายในทางแพ่งนี้จะหมดอายุความเมื่อพ้น 3 ปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลที่ต้องรับผิด หรือเมื่อพ้น 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

¹⁰⁴ มาตรา 78 วรรคหนึ่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹⁰⁵ มาตรา 78 วรรคสอง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

10.4 โทษทางอาญาของกรรมการหรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคล¹⁰⁶

ในกรณีที่บริษัทกระทำความผิดที่มีโทษทางอาญาตาม พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล¹⁰⁷ นอกจากโทษทางอาญาที่บริษัทอาจจะต้องรับแล้ว กรรมการ หรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทก็ต้องรับผิดชอบในโทษอาญาเช่นเดียวกับบริษัทด้วย หากพิสูจน์ว่า การกระทำความผิดดังกล่าวมีองค์ประกอบดังต่อไปนี้ได้

ผู้กระทำความผิด

- ก. กรรมการของบริษัท
- ข. ผู้จัดการของบริษัท หรือ
- ค. บุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท

การกระทำความผิด

- ก. การสั่งการ หรือการกระทำการของกรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท หรือ
- ข. การละเว้นไม่สั่งการ หรือไม่กระทำการ ในกรณีที่กรรมการ ผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทมีหน้าที่ต้องสั่งการหรือกระทำการ

และการกระทำตาม ก. หรือ ข. นั้นเป็นเหตุให้บริษัทกระทำความผิด

ตัวอย่าง

ผู้รับมอบอำนาจบริษัทสั่งให้นำข้อมูลส่วนบุคคลที่บริษัท เก็บรวบรวมมาภายใต้วัตถุประสงค์ในการพิจารณารับประกันภัยรถยนต์ ไปใช้ประมวลผลข้อมูลภายใต้วัตถุประสงค์เพื่อทำกิจกรรมส่งเสริมการขาย โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่นนี้เป็นกรณีที่บริษัท ผู้ควบคุมข้อมูลส่วนบุคคลกระทำความผิดโดยคำสั่งของบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท ดังนั้น ในกรณีนี้ทั้งบริษัท และผู้รับมอบอำนาจบริษัทจะต้องรับโทษทางอาญาที่เกี่ยวข้องตาม พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล

¹⁰⁶ มาตรา 81 พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล

¹⁰⁷ มาตรา 79 และมาตรา 80 พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล

10.5 โทษทางปกครอง

นอกจากโทษทางปกครองที่กำหนดไว้สำหรับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือตัวแทนของบุคคลดังกล่าว ตามที่ได้อธิบายไว้ที่ข้างต้นแล้ว บุคคลใด ๆ (ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงกรรมการ หรือผู้จัดการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัท) ที่ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือเจ้าพนักงานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล อาจต้องรับผิดหากบุคคลดังกล่าวกระทำการดังต่อไปนี้

- ไม่ปฏิบัติตามคำสั่งให้ส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมทั้งไม่มาชี้แจงข้อเท็จจริงต่อคณะกรรมการผู้เชี่ยวชาญ
- ไม่มาให้ข้อมูล หรือไม่ส่งเอกสารหรือหลักฐาน เกี่ยวกับการดำเนินการหรือการกระทำความผิดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่พนักงานเจ้าหน้าที่ตามหนังสือที่ได้แจ้งไปภายใต้อำนาจหน้าที่
- ไม่อำนวยความสะดวกตามสมควรแก่พนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่

ตัวอย่าง

- ในกรณีที่พนักงานเจ้าหน้าที่ได้รับคำสั่งจากศาลที่มีเขตอำนาจ เพื่อเข้าตรวจสอบและรวบรวมข้อเท็จจริง โดยยึด หรืออายัดหลักฐานที่พนักงานเจ้าหน้าที่มีเหตุอันควรเชื่อได้ว่าใช้เพื่อกระทำความผิด เช่นนี้ หากผู้จัดการสาขา ชัดขวางไม่ให้เจ้าพนักงานยึดเอาหลักฐานนั้นไป ผู้จัดการสาขาคงกล่าวอ้างจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท
- ในกรณีที่คณะกรรมการผู้เชี่ยวชาญสั่งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของบริษัทไปให้รายละเอียดเรื่องที่มีผู้ร้องเรียนบริษัท เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แต่ DPO ไม่ไปให้ข้อเท็จจริงโดยไม่มีเหตุผล ดังนี้ DPO อาจจะต้องระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท

ข้อสังเกต

- พนักงานเจ้าหน้าที่ จะเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลได้จะต้องเป็นไปตามเงื่อนไขที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด กล่าวคือ
 - ต้องมีคำสั่งอนุญาตของศาลที่มีเขตอำนาจ
 - เข้าไประหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก หรือในเวลาทำการของสถานที่นั้น

- แสดงบัตรประจำตัวต่อผู้ที่เกี่ยวข้อง
- โฆษทางปกครองในกรณีนี้ สามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองและกฎหมายว่าด้วยวิธีพิจารณาคดีปกครอง ตามลำดับ

บทที่ 11 ตัวอย่างร่างข้อความในเอกสารทางกฎหมายที่สำคัญ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

แบบ ข้อความ หรือสัญญาที่บรรจุไว้ในบทที่ 11 ของคู่มือนี้ เป็นเพียงตัวอย่างที่เตรียมขึ้นเพื่อเป็นแนวทางในการจัดเตรียมของบริษัท ซึ่งการนำไปใช้จะต้องได้รับการตรวจสอบ และตรวจทานโดยหน่วยงานต่างๆ ของบริษัท โดยเฉพาะอย่างยิ่งหน่วยงานที่กำกับดูแลด้านกฎหมาย กฎระเบียบ และด้านการปกป้องข้อมูลส่วนบุคคล เพื่อปรับแก้ หรือเพิ่มเติม ข้อความเพื่อให้เหมาะสมกับการดำเนินธุรกิจของแต่ละบริษัท

11.1 ตัวอย่างร่างข้อความแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล สำหรับลูกค้าและผู้มุ่งหวัง

Version: [ระบุVersion หรือวันที่อ้างอิงของนโยบาย]

นโยบายคุ้มครองข้อมูลส่วนบุคคลของ[ชื่อบริษัท]

[ระบุชื่อบริษัท] (“บริษัท”) และบริษัทในเครือหรือบริษัทในกลุ่มบริษัท [ชื่อบริษัท] (“กลุ่มบริษัท”) (เรียกรวมกันว่า “เรา” “พวกเรา” “ของเรา”) ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของเรา เกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย (“การประมวลผล”) ข้อมูลส่วนบุคคลของท่าน เราจึงได้จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้นมาเพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

1. บทนิยาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายถึง ข้อมูลตามที่กำหนดไว้ใน มาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

“พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล” หมายถึง พระราชบัญญัติคຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลຳดับรองที่อาศัยอำนาจ พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล ในการตราขึ้น และตามที่มีการแก้ไขเป็นครั้งคราว

“คณะกรรมการ” หมายถึง คณะกรรมการคຸ້ມครองข้อมูลส่วนบุคคล

2. ข้อมูลส่วนบุคคลใดบ้างที่เราจะเก็บรวบรวม

เราจะประมวลผลข้อมูลส่วนบุคคล ซึ่งอาจรวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวของท่าน ดังต่อไปนี้

2.1 ข้อมูลส่วนบุคคลทั่วไป

- (1) ข้อมูลส่วนบุคคลที่เกี่ยวกับท่านเป็นการทั่วไป เช่น ชื่อ-นามสกุล เลขบัตรประจำตัวประชาชน วันเกิด อายุ อาชีพ เพศ สถานภาพทางการสมรส รูปภาพ หมายเลขโทรศัพท์บ้าน หมายเลขโทรศัพท์เคลื่อนที่ ที่อยู่ตามทะเบียนบ้าน ที่อยู่เพื่อจัดส่งไปรษณีย์ เลขที่หนังสือเดินทาง อีเมล เสียงสนทนา และรายละเอียดข้อมูลติดต่ออื่น ๆ
- (2) ข้อมูลเกี่ยวกับการทำงานของท่าน เช่น ตำแหน่งงาน สถานที่ทำงาน ประวัติเกี่ยวกับการทำงานของท่าน ซึ่งอาจรวมถึงชื่อและที่อยู่ของนายจ้างของท่าน
- (3) ข้อมูลทางการเงิน เช่น รายได้ แหล่งที่มาของรายได้ เลขบัญชีธนาคาร ข้อมูลเกี่ยวกับภาษี รายละเอียดเกี่ยวกับการเคลื่อนไหวของบัญชีธนาคาร รายละเอียดเกี่ยวกับเงินกู้ ข้อมูลเกี่ยวกับการลงทุน รายละเอียดเกี่ยวกับบัตรเครดิต และรายละเอียดหรือข้อมูลเกี่ยวกับการชำระเงินอื่น ๆ
- (4) รายละเอียดผลิตภัณฑ์และ/หรือบริการต่าง ๆ ได้แก่ รายละเอียดผลิตภัณฑ์และ/หรือบริการต่าง ๆ ที่ท่านเคยซื้อจากเรา หรือผู้ประกอบการธุรกิจประกันภัยอื่น ๆ เช่น หมายเลขกรมธรรม์ จำนวนเงินเอาประกัน การเปลี่ยนแปลง/การทำธุรกรรมเกี่ยวกับกรมธรรม์ วิธีการจ่ายเบี้ยประกันภัย ประวัติการชำระเบี้ยประกันภัย หรือประวัติเกี่ยวกับการกู้ยืมเงิน ผู้รับประโยชน์ การเรียกร้องค่าสินไหมทดแทน รวมถึงการใช้สิทธิต่าง ๆ ภายใต้กรมธรรม์ หรือผลิตภัณฑ์ หรือบริการอื่น ๆ ของเรา หรือผู้ประกอบการธุรกิจประกันภัยอื่น ๆ

- (5) **สถานะทางกฎหมาย** เช่น สถานะเกี่ยวกับการฟอกเงิน สถานะเกี่ยวกับการสนับสนุนเงินแก่การก่อการร้าย ภาวะล้มละลาย สถานะตามกฎหมายสหรัฐอเมริกาว่าด้วยการป้องกันมิให้บุคคลธรรมดาและนิติบุคคลที่มีสถานะเป็นบุคคลอเมริกันหลีกเลี่ยงภาษี (Foreign Account Tax Compliance Act: FATCA)
- (6) **ข้อมูลทางเทคนิค และกิจกรรมส่วนบุคคล/ลักษณะการใช้งานที่ท่านชอบ** เมื่อท่านใช้เว็บไซต์ แอปพลิเคชันของเรา และอาจรวมถึงแพลตฟอร์มสื่อสังคมออนไลน์ของผู้ให้บริการอื่น เช่น ชื่อเรียกตัวตนเฉพาะของลูกค้าที่ใช้บนแพลตฟอร์มสื่อสังคมออนไลน์ IP Address คุกกี้ (Cookies) ประเภทและเวอร์ชันของเบราว์เซอร์ การตั้งค่าช่วงเวลา ประเภทของปลั๊กอินในเบราว์เซอร์ ระบบปฏิบัติการและแพลตฟอร์มข้อมูลผู้ใช้ (User Profile) ข้อมูลเกี่ยวกับอุปกรณ์ ซึ่งรวมถึงข้อมูลเกี่ยวกับอุปกรณ์เคลื่อนที่ ข้อมูลเครือข่ายไร้สายและข้อมูลเครือข่ายทั่วไป

2.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

บริษัทอาจมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลสุขภาพ ข้อมูลความพิการ ประวัติอาชญากรรม ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดในลักษณะเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

[โปรดระบุข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมให้ครบถ้วน]

ในกรณีที่บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อการเข้าทำสัญญา ประกันภัย การปฏิบัติตามสัญญา หรือการปฏิบัติหน้าที่ตามกฎหมาย หากท่านไม่ให้ข้อมูลส่วนบุคคลที่จำเป็นต่อการดำเนินงานของบริษัท บริษัทอาจไม่สามารถดำเนินการตามวัตถุประสงค์ที่ระบุไว้ในนโยบายฉบับนี้หรือให้บริการแก่ท่านได้อย่างเต็มรูปแบบ หรือท่านอาจไม่สามารถใช้บริการของบริษัทได้อย่างเหมาะสม หรืออาจส่งผลกระทบต่อการใช้บริการตามกฎหมายใด ๆ ที่บริษัทหรือท่านมีหน้าที่ต้องปฏิบัติตาม

3. เราเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเมื่อใด

เราอาจเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยวิธีต่อไปนี้

- (1) เมื่อท่านแสดงเจตนาจะซื้อหรือใช้ประกันภัยส่วนบุคคล ประกันภัยกลุ่ม และ/หรือเมื่อท่านเข้าถึงหรือใช้เว็บไซต์ หรือแอปพลิเคชัน และ/หรือบริการต่าง ๆ ทางออนไลน์ บนอุปกรณ์เคลื่อนที่หรือทางโทรศัพท์ หรือบริการอื่น ๆ ของเรา (“ผลิตภัณฑ์” หรือ“บริการ”)
- (2) เมื่อท่านส่งเอกสารและใบคำขอเอาประกันภัยเพื่อซื้อหรือใช้ หรือเมื่อท่านให้ข้อมูล ขณะที่พิจารณาจะซื้อหรือใช้ ผลิตภัณฑ์หรือบริการต่าง ๆ ของเรา
- (3) เมื่อท่านติดต่อสื่อสารกับเรา ไม่ว่าจะเป็นการสื่อสารเป็นหนังสือหรือวาจา โดยไม่คำนึงว่าฝ่ายใดจะเป็นผู้ติดต่อฝ่ายนั้นก่อนหรือไม่ก็ตาม
- (4) เมื่อท่านส่งคำร้องขอให้มีการเปลี่ยนแปลงหรือปรับปรุงผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ หรือคำร้องขออื่นใดเกี่ยวกับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ รวมถึงการส่งแบบฟอร์มและเอกสารเกี่ยวกับการขอรับบริการที่เกี่ยวกับผลิตภัณฑ์ของเรา
- (5) เมื่อท่านติดต่อกับบุคลากร เจ้าหน้าที่บริการลูกค้า พนักงานขาย ตัวแทนประกันภัย นายหน้าคนกลางประกันภัย ผู้รับจ้าง คู่ค้า ผู้ให้บริการ ผู้รับมอบอำนาจ ผู้กระทำการแทน หรือบุคคลอื่นหรือหน่วยงานอื่นที่เกี่ยวข้องของบริษัท (เรียกรวมกันว่า “บุคลากรและคู่ค้าของบริษัท”) ผ่านทางเว็บไซต์ แอปพลิเคชัน สื่อสังคมออนไลน์ โทรศัพท์ อีเมล การพบปะกันโดยตรง การสัมภาษณ์ ข้อความสั้น (SMS) โทรสาร ไปรษณีย์ หรือโดยวิธีการอื่นใด
- (6) เมื่อเราได้รับการแนะนำเกี่ยวกับท่าน หรือเมื่อเราเก็บรวบรวมข้อมูลส่วนบุคคลจากบุคลากรและคู่ค้าของเรา
- (7) เมื่อท่านส่งข้อมูลส่วนบุคคลให้แก่เราเพื่อเข้าร่วมในกิจกรรมทางการตลาด การประกวด การจับฉลากชิงโชค งานอีเว้นท์ หรือการแข่งขันต่าง ๆ ที่จัดขึ้นโดยหรือในนามของเรา และ/ หรือบุคลากรและคู่ค้าของเรา
- (8) เมื่อเราได้รับข้อมูลส่วนบุคคลจากบุคคลภายนอกเกี่ยวกับท่าน ซึ่งรวมถึงแต่ไม่จำกัดเพียงการได้รับข้อมูลจากการตรวจสอบจากแหล่งข้อมูลที่เป็นสาธารณะ แหล่งข้อมูลส่วนตัว หรือแหล่งข้อมูลเชิงพาณิชย์ เว็บไซต์ แหล่งข้อมูลสื่อสังคมออนไลน์ ผู้ให้บริการข้อมูล (Data Providers) แหล่งข้อมูลทางการแพทย์ สถานบริการสาธารณสุข โรงพยาบาล แพทย์ บุคลากรผู้ประกอบวิชาชีพสาธารณสุขอื่น ผู้ประกอบธุรกิจประกันภัยอื่น สมาคมหรือสมาคมพันธมิตรของธุรกิจที่

เกี่ยวข้องกับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ ใบคำขอเอาประกันสำหรับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ การรับประกันความเสี่ยงของผลิตภัณฑ์ที่ท่านซื้อ การร้องเรียนเกี่ยวกับผลิตภัณฑ์ และ/หรือผลิตภัณฑ์และบริการของเรา ที่ซื้อหรือใช้โดยท่าน (“แหล่งข้อมูลที่เป็นบุคคลภายนอก”)

- (9) เมื่อเราได้รับข้อมูลส่วนบุคคลจากบุคคลภายนอกเกี่ยวกับท่านเพื่อวัตถุประสงค์ในการปฏิบัติตามกฎหมายและเพื่อวัตถุประสงค์เกี่ยวกับการกำกับดูแลในประการอื่น ๆ ตลอดจนเพื่อวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมาย เช่น บริษัทอาจได้รับข้อมูลส่วนบุคคลของท่านจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)

[โปรดระบุแหล่งที่มาของการเก็บรวบรวมข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

เมื่อท่านให้ข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับบุคคลภายนอกแก่เรา (ซึ่งบุคคลภายนอกดังกล่าวรวมถึงแต่ไม่จำกัดเพียงผู้เอาประกันภัย สมาชิกในครอบครัว ผู้ชำระเงินตามกรมธรรม์ หรือผู้รับประโยชน์) ท่านต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขอความยินยอมหรือแจ้งนโยบายฉบับนี้แก่บุคคลที่สามในนามของบริษัท ทั้งนี้ ท่านรับรองและรับประกันความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมทั้งรับรองและรับประกันว่าท่านได้แจ้งให้บุคคลเหล่านั้นทราบอย่างครบถ้วนแล้วเกี่ยวกับรายละเอียดตามนโยบายฉบับนี้

4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

เราจะประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ดังต่อไปนี้

- (1) เพื่อดำเนินการเกี่ยวกับการเข้าทำสัญญาประกันภัย หรือการดำเนินการตามสัญญา กล่าวคือ (ก) เพื่อเสนอขาย ขาย จัดให้ บริหารจัดการ ดำเนินการ ปฏิบัติตามขั้นตอนกระบวนการ และจัดการเกี่ยวกับผลิตภัณฑ์และ/ หรือบริการของเราให้แก่ท่าน (ข) เพื่อปฏิบัติตามขั้นตอนกระบวนการ จัดการ ทำให้แล้วเสร็จ ซึ่งการให้บริการ หรือผลิตภัณฑ์ของเรา และการแนะนำผลิตภัณฑ์และบริการที่เหมาะสมให้แก่ท่าน การปฏิบัติตามขั้นตอนกระบวนการเกี่ยวกับใบคำขอเอาประกันสำหรับผลิตภัณฑ์ การจัดการเกี่ยวกับผลิตภัณฑ์ที่ท่านซื้อ การเก็บเบี้ยประกันภัย และเงินค้ำชำระจากท่าน การสืบสวน วิเคราะห์ ประมวลผล การเวนคืนกรมธรรม์ และการจ่ายค่าสินไหมทดแทน/ การจ่ายผลประโยชน์ตามกรมธรรม์ภายใต้กรมธรรม์ของท่าน และการต่ออายุ ปรับปรุงแก้ไข ยกเลิกกรมธรรม์ของท่าน ตลอดจนถึงการใช้สิทธิใด ๆ ภายใต้กรมธรรม์ของท่าน ซึ่งรวมถึงสิทธิในการรับช่วงสิทธิ และสิทธิที่ได้รับช่วงมาด้วย (หากมี)

(2) เพื่อดำเนินการตามความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท กล่าวคือ

- (ก.) เพื่อการจัดการเกี่ยวกับการประกันภัยของบริษัท เช่น การออกแบบผลิตภัณฑ์หรือบริการใหม่ของเรา หรือการเสริมเพิ่มเติมผลิตภัณฑ์หรือบริการที่มีอยู่ของเรา การดำเนินการเพื่อทำประกันภัยสำหรับผลิตภัณฑ์หรือบริการของเราให้แก่ท่าน
- (ข.) เพื่อการติดต่อสื่อสารกับท่าน ซึ่งรวมถึงการสื่อสารข้อมูลเกี่ยวกับการจัดการและข้อมูลอื่น ๆ เกี่ยวกับผลิตภัณฑ์หรือบัญชีใด ๆ ที่ท่านอาจมีกับเรา การให้การสนับสนุนทางเทคนิคเกี่ยวกับเว็บไซต์และแอปพลิเคชันของเรา หรือการสื่อสารเกี่ยวกับการเปลี่ยนแปลงใด ๆ ที่จะมีขึ้นต่อนโยบายความเป็นส่วนตัวส่วนบุคคลฉบับนี้ในอนาคต
- (ค.) เพื่อการป้องกันการฉ้อโกง/ฉ้อฉล เช่น การสืบสวนหรือป้องกันการกระทำที่เกี่ยวกับการฉ้อโกง การปกปิดข้อความจริง และการกระทำผิดอื่น ๆ ไม่ว่าจะเป็นการกระทำผิดจริงหรือการกระทำที่สงสัยว่าจะเป็นการกระทำผิด โดยเฉพาะอย่างยิ่งเพื่อการติดต่อสื่อสารกับบริษัทต่าง ๆ ในธุรกิจบริการทางการเงินและการประกันภัย ตลอดจนเพื่อการติดต่อสื่อสารกับหน่วยงานกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง
- (ง.) เพื่อการปรับโครงสร้างของบริษัท เช่น เพื่อวัตถุประสงค์ในการปรับโครงสร้างองค์กรของบริษัท และเพื่อการทำธุรกรรมของบริษัท รวมถึงการซื้อ หรือขายธุรกิจไม่ว่าส่วนใดส่วนหนึ่งของบริษัท (หากมี)
- (จ.) เพื่อให้บริการช่องทางการสื่อสารทางอิเล็กทรอนิกส์ เช่น เพื่อให้ท่านสามารถเข้าถึงเนื้อหาในเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ หรือบริการอย่างใดอย่างหนึ่งเป็นการเฉพาะ โดยเราอาจประมวลผลพฤติกรรมการใช้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ เพื่อการวิเคราะห์การใช้งานเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ของท่าน และการทำความเข้าใจลักษณะการใช้งานที่ท่านชอบ เพื่อจัดทำให้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้นตอบสนองอย่างเหมาะสมกับท่านโดยเฉพาะ เพื่อการประเมินหรือดำเนินการ และการปรับปรุงเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้น หรือผลิตภัณฑ์และ/หรือบริการของเรา การแก้ไขปัญหาต่าง ๆ การแนะนำผลิตภัณฑ์และ/หรือบริการที่เกี่ยวข้อง และการจัดโฆษณาบนเว็บไซต์ แอปพลิเคชัน และช่องทางอื่น ๆ ตามกลุ่มเป้าหมาย
- (ฉ.) เพื่อการบริหารจัดการข้อมูล เช่น เพื่อวัตถุประสงค์ในการบริหารจัดการ จัดเก็บ บันทึก สำรอง หรือทำลายข้อมูลส่วนบุคคล

(ข.) เพื่อพัฒนาการผลิตภัณฑ์และการให้บริการของเรา เช่น การตรวจสอบและเพิ่มคุณภาพ รวมทั้งการฝึกอบรม เมื่อมีการบันทึกการติดต่อสื่อสารของเรา

(ข.) เพื่อดำเนินการส่งเสริมการขาย เช่น การดำเนินการให้ข้อมูลเกี่ยวกับ ผลิตภัณฑ์ และการบริการที่เหมาะสมแก่ท่าน ซึ่งอาจรวมถึงการให้คำแนะนำและข้อมูลในเรื่องต่าง ๆ ซึ่งรวมถึงการประกัน ตลอดจนถึงกิจกรรมส่งเสริมการขายผลิตภัณฑ์และการบริการ เช่น โปรแกรมให้รางวัล/ให้ผลประโยชน์สำหรับการเป็นลูกค้าที่มีความภักดีต่อแบรนด์/ให้สิทธิพิเศษ กิจกรรมการกุศล/กิจกรรมที่ไม่หวังผล และการจัดกิจกรรมทางการตลาด งานอีเว้นท์ และกิจกรรมอื่น ๆ ซึ่งท่านเลือกที่จะเข้าร่วม

(ณ.) เพื่อการปฏิบัติตามนโยบายของบริษัท เพื่อดำเนินการให้เป็นไปตามข้อกำหนดภายใต้นโยบายภายในของเราที่ยึดถือปฏิบัติ

(3) เพื่อการวิเคราะห์และจัดทำสถิติ เช่น การทำวิจัยทางการตลาด การวิเคราะห์ข้อมูลขั้นสูง และการทำวิจัยเชิงสถิติหรือคณิตศาสตร์ประกันภัย การรายงานหรือการประเมินผลทางการเงินที่จัดทำขึ้นโดยบริษัท กลุ่มบริษัท บุคลากรและคู่ค้าของบริษัท หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับเรา

(4) เพื่อการปฏิบัติตามกฎหมาย เช่น การดำเนินการใด ๆ (ก) เพื่อดำเนินการตามกฎหมาย หรือการตรวจสอบธุรกิจของเรา ไม่ว่าจะเป็นการตรวจสอบภายใน หรือการตรวจสอบจากบุคคลภายนอก (ข) เพื่อดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมาย กฎ ระเบียบ ข้อตกลง หรือนโยบายที่ใช้บังคับ ซึ่งกำหนดขึ้นโดยหน่วยงานกำกับดูแลของรัฐ หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย หน่วยงานรัฐ หน่วยงานที่มีหน้าที่ระงับข้อพิพาท สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยหรือหน่วยงานที่ดูแลธุรกิจประกันภัย ไม่ว่าหน่วยงานใดก็ตาม (ค) เพื่อวัตถุประสงค์ของการบังคับใช้กฎหมาย หรือการให้ความช่วยเหลือ ให้ความร่วมมือ การสืบสวนโดยเราหรือในนามของเรา โดยเจ้าหน้าที่ตำรวจ หรือโดยหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศ และการดำเนินการตามหน้าที่ในการรายงาน และข้อกำหนดต่าง ๆ ตามที่กฎหมายกำหนด หรือตามที่มีการตกลงเห็นชอบกับหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศหรือเขตการปกครองใด ๆ หรือการดำเนินการตามคำสั่งโดยชอบด้วยกฎหมายของพนักงานเจ้าหน้าที่ หรือหน่วยงานของรัฐ และ (ง) เพื่อสนับสนุนการกำกับดูแลและส่งเสริมธุรกิจประกันภัยตามกฎหมายว่าด้วยคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยและกฎหมายว่าด้วยการประกันวินาศภัยของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ตามนโยบายคุ้มครองข้อมูลส่วนบุคคล

บุคคลของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ซึ่งสามารถ
ตรวจสอบได้ที่เว็บไซต์ (<https://www.oic.or.th>)

- (5) **อื่น ๆ** กล่าวคือ เพื่อการดำเนินการอื่น ๆ ที่จำเป็น ซึ่งเกี่ยวข้องกับวัตถุประสงค์ใด ๆ ข้างต้น
เว้นแต่กฎหมายและกฎระเบียบที่ใช้บังคับ รวมถึง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จะอนุญาตให้
กระทำเป็นอย่างอื่น เราจะแจ้งและขอความยินยอมจากท่านหากเราประสงค์จะใช้ข้อมูลส่วนบุคคล
ของท่านเพื่อวัตถุประสงค์อื่นใดนอกเหนือไปจากที่ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้
หรือนอกเหนือไปจากวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับนโยบายคุ้มครองข้อมูลส่วนบุคคลนี้

[โปรดระบุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

5. บุคคลใดบ้างที่อาจได้รับข้อมูลส่วนบุคคลของท่านจากบริษัท

ในการดำเนินการตามวัตถุประสงค์ต่าง ๆ ข้างต้น เราอาจเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่
บุคคลต่าง ๆ ตามที่ระบุด้านล่างนี้ โดยเราจะดำเนินใด ๆ ที่จำเป็นเพื่อคุ้มครองข้อมูลส่วนบุคคลของ
ท่านตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- (1) บุคคลที่เป็นคู่ค้า พันธมิตรของบริษัท หรือบุคคลภายนอกที่มีความเกี่ยวข้องกับผลิตภัณฑ์
ประกันภัยที่มีการเสนอขายให้แก่ท่าน หรือผลิตภัณฑ์ที่ท่านอาจสนใจ เช่น บริษัทประกันภัยต่อ
บริษัทจัดการการลงทุน ธนาคาร สถาบันการเงิน สถาบันจัดอันดับความน่าเชื่อถือ
- (2) ผู้ถือกรรมธรรม์ ในกรณีของผลิตภัณฑ์ประกันภัยแบบกลุ่ม
- (3) บุคคลผู้ดำเนินการเชิญชวน ชักชวน ชี้ช่อง จัดการให้ทำ เสนอขาย ขาย จัดจำหน่าย หรือ
ให้บริการเกี่ยวกับผลิตภัณฑ์และ/หรือบริการที่เสนอโดยบริษัท หรือบริษัทในกลุ่มบริษัทให้แก่
ท่าน ได้แก่ ตัวแทนประกันภัย นายหน้าประกันภัย รวมถึงบุคลากรของนายหน้าประกันภัยซึ่ง
เป็นนิติบุคคล
- (4) บุคลากรและคู่ค้าของเราไม่ว่ารายใดก็ตาม ซึ่งให้บริการเกี่ยวกับการจัดการต่าง ๆ หรือการ
ให้บริการประมวลผลข้อมูลส่วนบุคคล ได้แก่ บริการเกี่ยวกับกระบวนการทางธุรกิจ บริการ
เกี่ยวกับการชำระเงิน การทวงหนี้ หรือบริการโทรคมนาคม บริการด้านเทคโนโลยี บริการ
คลาวด์ บริการจัดหาผู้รับจ้างปฏิบัติงาน บริการคอลเซ็นเตอร์ บริการจัดเก็บของ การ

ดำเนินการเกี่ยวกับเอกสาร บริการเก็บบันทึกข้อมูล บริการสแกนเอกสาร บริการรับส่ง ไปรษณีย์ บริการจัดพิมพ์ บริการส่งพัสดุหรือบริการรับส่งพัสดุโดยพนักงานรับส่งพัสดุ บริการ วิเคราะห์ข้อมูล บริการทำการตลาด บริการทำการวิจัย บริการบริหารจัดการเหตุฉุกเฉิน บริการทางกฎหมาย หรือบริการอื่น ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท หรือการจัดให้ มีการบริหารจัดการ การดำเนินการ การปฏิบัติตามขั้นตอน หรือการจัดการต่าง ๆ เกี่ยวกับ ผลิตภัณฑ์หรือบริการของบริษัทให้แก่ท่าน

- (5) ผู้ให้บริการก่อนรับการประกันภัย เช่น ผู้สำรวจภัยก่อนรับประกันภัย เป็นต้น
- (6) ผู้ให้บริการเพื่อخذใช้สินไหมทดแทน เช่น ผู้สำรวจอุบัติเหตุ ศูนย์บริการรถยนต์ อยู่ โรงพยาบาล เป็นต้น
- (7) ผู้ประกอบธุรกิจประกันภัยรายอื่น ๆ
- (8) สมาคมหรือสมาพันธ์ในภาคธุรกิจประกันภัย
- (9) หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย คณะกรรมการต่าง ๆ ที่จัดตั้งขึ้นตามกฎหมาย หน่วยงาน รัฐบาลหรือหน่วยงานกำกับดูแล หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือบุคคลอื่นใดในประเทศที่ บริษัท หรือบริษัทในกลุ่มบริษัทต้องเปิดเผยข้อมูลให้ (ก) ตามหน้าที่ตามกฎหมายและ/ หรือ ตามหน้าที่ในการปฏิบัติตามกฎระเบียบในประเทศไทย และอาจรวมถึงหน่วยงานของรัฐใน ประเทศที่กลุ่มบริษัทตั้งอยู่ หรือ (ข) ตามข้อตกลง หรือนโยบายระหว่างบริษัทในกลุ่มบริษัท กับรัฐ หน่วยงานกำกับดูแล หรือบุคคลอื่น ๆ ที่เกี่ยวข้อง
- (10) บริษัทใด ๆ ในกลุ่มบริษัท
- (11) ผู้ให้คำปรึกษาของบริษัท ซึ่งเป็นผู้ประกอบวิชาชีพ เช่น หนายความ แพทย์ ผู้ตรวจสอบบัญชี หรือที่ปรึกษา
- (12) บุคคลหรือหน่วยงานใด ๆ ที่ท่านให้ความยินยอมให้เปิดเผยข้อมูลส่วนบุคคลของท่านต่อบุคคล หรือหน่วยงานนั้น ๆ ได้
- (13) ผู้เข้าทำธุรกรรม หรือจะเข้าทำธุรกรรมกับบริษัทโดยข้อมูลส่วนบุคคลของท่านอาจเป็นส่วนหนึ่ง ของการซื้อขาย หรือเป็นส่วนหนึ่งของการเสนอซื้อหรือเสนอขายของกิจการของบริษัท (หากมี)

(14) บุคคลหรือหน่วยงานอื่นใดที่ได้รับอนุญาตตามกฎหมายที่ใช้บังคับ

[โปรดระบุบุคคลที่อาจได้รับข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

6. การโอนข้อมูลไปยังต่างประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัท หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่ในประเทศไทยหรือนอกประเทศไทย ทั้งนี้ ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท เราจะดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัทที่ได้รับการอนุมัติจากคณะกรรมการ (หากมี)

7. การเก็บรักษาข้อมูลส่วนบุคคล

เราจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ トラバเท่าที่จำเป็นต้องเก็บเพื่อการดำเนินการให้บรรลุตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของท่านตามที่ระบุข้างต้น ทั้งนี้บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไม่เกิน 10 ปี นับแต่วันที่ท่านสิ้นสุดความสัมพันธ์ หรือการติดต่อครั้งสุดท้ายกับเรา บริษัทอาจเก็บรักษาข้อมูลส่วนบุคคลของท่านนานกว่าที่กำหนดหากกฎหมายอนุญาต

เราจะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อทำการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่ไม่สามารถระบุตัวท่าน ตามระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลข้างต้น

8. การใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม

บริษัทมีสิทธิในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านที่บริษัทได้เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลมีผลใช้บังคับต่อไปตามวัตถุประสงค์เดิม หากท่านไม่ประสงค์ที่จะให้บริษัทเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวต่อไป ท่านสามารถแจ้งบริษัทเพื่อขอถอนความยินยอมของท่านตามหลักเกณฑ์ที่กฎหมายกำหนดได้ที่ [โปรดระบุช่องทางการขอถอนความยินยอม]

9. การรักษาความปลอดภัย

บริษัทมีการใช้มาตรการรักษาความปลอดภัยภายในบริษัทและการใช้บังคับนโยบายอย่างเข้มงวดในการเก็บรักษาข้อมูลส่วนบุคคลของท่านให้ปลอดภัย ซึ่งรวมถึงการเข้ารหัสข้อมูล และมาตรการป้องกันการเข้าถึงข้อมูล โดยบริษัทกำหนดให้บุคลากรของบริษัทและผู้รับจ้างภายนอกจะต้องปฏิบัติตามมาตรฐานและนโยบายความเป็นส่วนตัวส่วนบุคคลที่เหมาะสม รวมถึงจะต้องจัดให้มีการดูแลรักษาข้อมูลและมีมาตรการที่เหมาะสมในการใช้หรือการส่งหรือโอนข้อมูลส่วนบุคคลของท่าน

10. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

- (1) เพิกถอน หรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านที่ได้ให้ไว้กับเรา
- (2) ขอเข้าถึง ขอรับสำเนา หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เกี่ยวกับท่านโดยท่านไม่ได้ให้ความยินยอม
- (3) ขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับท่าน หรือขอให้ส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น
- (4) คัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

(ก.) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เนื่องจากเป็นการจำเป็นเพื่อประโยชน์สาธารณะ หรือการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย ตามมาตรา 24 (4) หรือ (5) แห่งพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เว้นแต่เราสามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(ข.) การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

(ค.) การประมวลผลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะของเรา

- (5) ขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามหลักเกณฑ์ที่กฎหมายกำหนด
- (6) ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านตามหลักเกณฑ์ที่กฎหมายกำหนด
- (7) ขอให้แก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด หากเราไม่สามารถดำเนินการให้ได้ ท่านมีสิทธิขอบันทึกคำร้องขอของท่านพร้อมเหตุผลในการดำเนินการได้ตามหลักเกณฑ์ที่กฎหมายกำหนด

ทั้งนี้ เราขอสงวนสิทธิ์ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและตามหลักเกณฑ์ที่กฎหมายกำหนด อย่างไรก็ตาม เราอาจเรียกเก็บค่าใช้จ่ายตามสมควรเพื่อดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้นด้วย

นอกจากสิทธิของท่านตามที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของบริษัทต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

11. การแก้ไขเปลี่ยนแปลงนโยบายฉบับนี้

บริษัทขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฉบับนี้ บริษัทจะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายให้ท่านทราบ และ/หรือจะขอความยินยอมจากท่าน (หากกฎหมายกำหนดให้ต้องได้รับความยินยอม)

12. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเราที่

รายละเอียดของบริษัท

ชื่อ: [ชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับเรื่องขอใช้
สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท [ระบุชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับ
เรื่องขอใช้สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

11.2 ตัวอย่างร่างข้อความแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล สำหรับคู่ค้า (รวมทั้งนายหน้าประกันวินาศภัย)

Version: [ระบุVersion หรือวันที่อ้างอิงของนโยบาย]

นโยบายคุ้มครองข้อมูลส่วนบุคคลของ[ชื่อบริษัท]

[ชื่อบริษัท] (“บริษัท”) และบริษัทในเครือหรือบริษัทในกลุ่มบริษัท [ชื่อบริษัท] (“กลุ่มบริษัท”) (เรียกรวมกันว่า “เรา” “พวกเรา” “ของเรา”) ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของเราเกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย (“การประมวลผล”) ข้อมูลส่วนบุคคลของท่าน บริษัทจึงได้จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (“นโยบาย”) ฉบับนี้ขึ้นเพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”)

1. บทนิยาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายถึง ข้อมูลตามที่กำหนดไว้ในมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่อาศัยอำนาจ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ในการตราขึ้น และตามที่มีการแก้ไขเป็นครั้งคราว

“คณะกรรมการ” หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2. ข้อมูลส่วนบุคคลใดบ้างที่เราจะเก็บรวบรวม

ข้อมูลส่วนบุคคลที่เราอาจเก็บรวบรวมประกอบไปด้วยข้อมูลของท่านดังต่อไปนี้

2.1 กรณีที่ท่านดำเนินการในนามของตนเอง

- (1) ข้อมูลที่ใช้ระบุตัวบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ตามทะเบียนบ้าน ที่อยู่ปัจจุบัน หมายเลขโทรศัพท์บ้านหรือมือถือ หรือรายละเอียดการติดต่ออื่น ๆ เพศ สัญชาติ สถานภาพการสมรส วันเกิด เลขที่หนังสือเดินทาง/บัตรประจำตัวประชาชน
- (2) ข้อมูลเกี่ยวกับคุณวุฒิและประวัติการทำงานของท่าน เช่น คุณวุฒิการศึกษาจากโรงเรียนหรือมหาวิทยาลัย รวมถึง หนังสือรับรองและหนังสืออ้างอิงจากสถาบันการศึกษา
- (3) ข้อมูลเกี่ยวกับการสมัครงานของท่าน เช่น ประวัติส่วนตัว ข้อมูลการสัมภาษณ์งาน และหลักฐานหรือหนังสืออ้างอิงต่าง ๆ ฯลฯ
- (4) รายละเอียดการทำงานพื้นฐาน เช่น รายละเอียดสถานที่ทำงานของท่าน หมายเลขใบอนุญาตตัวแทนประกันภัย/ นายหน้าประกันภัย รายละเอียดหน่วยงานต้นสังกัด ตำแหน่ง สายการบังคับบัญชา และข้อตกลงและเงื่อนไขของการเป็นตัวแทน/ นายหน้าประกันวินาศภัย
- (5) ประวัติเกี่ยวกับประสิทธิภาพการทำงาน รวมถึง การประเมินผลการปฏิบัติงาน รางวัลที่เคยได้รับ ประวัติการถูกร้องเรียน บันทึกการสอบสวน การถูกพักสัญญาตัวแทน/นายหน้าประกันวินาศภัย และโทษทางวินัย รวมถึงการตรวจสอบและการประเมินความเสี่ยง
- (6) ข้อมูลเกี่ยวกับผลประโยชน์และค่าตอบแทน เช่น รายละเอียดเกี่ยวกับค่าบำเหน็จ และ/ หรือผลประโยชน์อื่น ๆ ที่ท่านได้รับ เลขบัญชีธนาคาร
- (7) ประวัติเกี่ยวกับการล้มละลาย การฟอกเงิน หรือการให้การสนับสนุนทางการเงินแก่ผู้ก่อการร้าย

2.2 กรณีที่ท่านดำเนินการแทนหรือเพื่อบุคคลของท่าน

กรณีที่คู่สัญญาของเราเป็นนิติบุคคล เราอาจประมวลข้อมูลส่วนบุคคลของท่านในฐานะที่ท่านเป็นพนักงาน ผู้รับจ้าง หรือผู้มีอำนาจกระทำการแทนนิติบุคคลของท่าน

- (1) ข้อมูลที่ใช้ระบุตัวบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ตามทะเบียนบ้าน ที่อยู่ปัจจุบัน หมายเลขโทรศัพท์บ้านหรือมือถือ อีเมล เลขที่หนังสือเดินทางหรือเลขบัตรประจำตัวประชาชน
- (2) ข้อมูลของท่านที่ปรากฏในหนังสือรับรองบริษัท บัญชีรายชื่อผู้ถือหุ้น หรือเอกสารเกี่ยวกับนิติบุคคลอื่นใดที่มีข้อมูลส่วนบุคคลของท่าน
- (3) ประวัติเกี่ยวกับการล้มละลาย การฟอกเงิน หรือการให้การสนับสนุนทางการเงินแก่ผู้ก่อการร้าย ประวัติอาชญากรรม เป็นต้น
- (4) ข้อมูลอื่นใดที่เราร้องขอจากนิติบุคคลของท่าน หรือจากท่านเพื่อใช้ในการประกอบการเข้าทำสัญญา การบริการ หรือการดำเนินการอื่นใดที่เกี่ยวข้อง ตามที่บริษัทได้แจ้งหรือร้องขอไปยังท่าน

ทั้งนี้ หากท่านดำเนินการเกี่ยวกับการเสนอขาย หรือกระทำการเป็นตัวแทนประกันภัย หรือนายหน้าประกันด้วย เราจะประมวลผลข้อมูลส่วนบุคคลของท่านตามรายละเอียดในข้อ 2.1 ด้วย

[โปรดระบุข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมให้ครบถ้วน]

ในกรณีที่บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อการเข้าทำสัญญา การปฏิบัติตามสัญญา หรือการปฏิบัติหน้าที่ตามกฎหมาย หากท่านไม่ให้ข้อมูลส่วนบุคคลที่จำเป็นต่อการดำเนินงานของบริษัท บริษัทอาจไม่สามารถดำเนินการตามวัตถุประสงค์ที่ระบุไว้ในนโยบายฉบับนี้ หรือดำเนินธุรกรรมกับท่านได้อย่างเต็มรูปแบบ หรืออาจส่งผลกระทบต่อการใช้บริการตามกฎหมายใด ๆ ที่บริษัทหรือท่านมีหน้าที่ต้องปฏิบัติตาม

เมื่อท่านให้ข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับบุคคลภายนอกแก่เรา (ซึ่งบุคคลภายนอกดังกล่าวรวมถึงแต่ไม่จำกัดเพียงผู้เอาประกันภัย สมาชิกในครอบครัว ผู้ชำระเงินตามกรมธรรม์ หรือผู้รับประโยชน์) ท่านต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขอความยินยอมหรือแจ้งนโยบายฉบับนี้แก่บุคคลที่สามในนามของบริษัท ทั้งนี้ ท่านรับรองและรับประกันความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมทั้งรับรองและรับประกันว่าท่านได้แจ้งให้บุคคลเหล่านั้นทราบอย่างครบถ้วนแล้วเกี่ยวกับรายละเอียดตามนโยบายฉบับนี้

3. เราเก็บรวบรวมข้อมูลส่วนบุคคลของท่านอย่างไร

โดยทั่วไปบริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยตรงจากท่าน เว้นแต่บางกรณีที่บริษัทอาจเก็บรวบรวมข้อมูลของท่านจากบุคคลอื่นที่แนะนำท่านให้เรา จากแหล่งข้อมูลสาธารณะ แหล่งข้อมูลเกี่ยวกับธุรกิจของท่าน หรือแหล่งข้อมูลทางการค้า

[โปรดระบุแหล่งที่มาของการเก็บรวบรวมข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

- (1) เราประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อการเข้าทำสัญญากับท่าน และเพื่อการปฏิบัติตามสิทธิหน้าที่ที่มีตามสัญญาที่เราเข้าทำกับท่าน
- (2) ในกรณีที่ท่านดำเนินการเป็นตัวแทนประกันวินาศภัย หรือนายหน้าประกันวินาศภัย ข้อมูลส่วนบุคคลของท่านจะถูกใช้เพื่อวัตถุประสงค์ในการบริหารจัดการธุรกิจตัวแทนและ/หรือนายหน้าประกันวินาศภัย รวมถึงแต่ไม่จำกัดอยู่เพียงการวางแผนกำลังคน การจ่ายผลประโยชน์ ค่าตอบแทน การคิดค่าตอบแทนที่จูงใจ ข้อเสนอ รางวัล การประเมินผลการปฏิบัติงานที่ การรายงานหรือตรวจสอบภายใน การวิเคราะห์ข้อมูล การแข่งขันทางการขาย ต่าง ๆ การติดต่อสื่อสาร การประกาศ การทำแบบสำรวจ สถิติ ตรวจสอบข้อร้องเรียนและประเด็นของการประพฤติดัวไม่เหมาะสม หรือเป็นส่วนหนึ่งของกระบวนการทางวินัย การตรวจสอบข้อมูลของท่านทางกฎหมาย ความสามารถในการทำงาน การร้องขอข้อมูลใด ๆ โดยรัฐบาลไม่ว่าจะเพื่อเหตุใด ตลอดจนเพื่อการประกอบกิจการของกลุ่มบริษัท ซึ่งรวมถึงแต่ไม่จำกัดเพียง จัดทำบันทึกข้อมูลตัวแทนประกันวินาศภัย การทำประกันภัย การตรวจสอบ การอ้างอิงและประวัติโดยสมาชิกใด ๆ ของกลุ่มบริษัทหรือบุคคลอื่น การหลีกเลี่ยงการขัดกันของผลประโยชน์ หรือหลีกเลี่ยงแนวโน้มที่จะเกิดการขัดกันของผลประโยชน์ และการตรวจสอบโดยสมาชิกใด ๆ ของกลุ่มบริษัท นอกจากนี้ ข้อมูลส่วนบุคคลของท่านยังอาจจะถูกใช้เพื่อวัตถุประสงค์เพื่อปฏิบัติตามกฎหมายและกฎเกณฑ์ที่ใช้บังคับ และการปฏิบัติตามข้อกำหนดของหน่วยงานกำกับดูแลตามกฎหมายทั้งในและนอกประเทศของท่าน แล้วแต่กรณี
- (3) เพื่อการปฏิบัติตามกฎหมาย รวมถึงแต่ไม่จำกัดเฉพาะประกาศ ระเบียบ และคำสั่งโดยชอบด้วยกฎหมายของหน่วยงานรัฐและเจ้าหน้าที่รัฐที่เกี่ยวข้อง

- (4) เพื่อสนับสนุนการกำกับดูแลและส่งเสริมธุรกิจประกันภัยตามกฎหมายว่าด้วยคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยและกฎหมายว่าด้วยการประกันวินาศภัยของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ซึ่งสามารถตรวจดูได้ที่เว็บไซต์ (<https://www.oic.or.th>)
- (5) เพื่อดำเนินการตามความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท รวมถึงเพื่อการก่อตั้ง ใช้ โต้แย้ง หรือดำเนินการตามสิทธิเรียกร้องของบริษัท การตรวจสอบและยืนยันตัวตนของท่าน การตรวจสอบประวัติก่อนและระหว่างเข้าทำสัญญา และอาจมีการตรวจสอบรายละเอียดดังกล่าวระหว่างระยะเวลาตามสัญญา หรือเพื่อการติดต่อ และการดำเนินธุรกิจของบริษัทตลอดระยะเวลาที่บริษัทยังมีความสัมพันธ์กับท่าน
- (6) เพื่อการวิเคราะห์และจัดทำสถิติ เช่น การทำวิจัยทางการตลาด การวิเคราะห์ข้อมูลขั้นสูง และการทำวิจัยเชิงสถิติหรือคณิตศาสตร์ประกันภัย การรายงานหรือการประเมินผลการดำเนินงานที่จัดทำขึ้นโดยบริษัท กลุ่มบริษัท บุคลากรและคู่ค้าของบริษัท หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับเรา

[โปรดระบุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

5. บุคคลใดบ้างที่อาจจะได้รับข้อมูลส่วนบุคคลของท่านจากบริษัท

เราอาจมีการเปิดเผย และ/หรือโอนข้อมูลส่วนบุคคลของท่านไปยังบุคคลดังต่อไปนี้ โดยที่บุคคลดังกล่าวอาจอยู่ในประเทศไทย หรือนอกประเทศไทยก็ได้

- (1) สมาชิกใด ๆ ของกลุ่มบริษัท
- (2) ตัวแทน/ นายหน้าประกันวินาศภัยของบริษัท
- (3) ที่ปรึกษาหรือผู้เชี่ยวชาญ ภายในหรือภายนอกของเรา เช่น ที่ปรึกษาทางกฎหมาย ผู้ตรวจสอบบัญชี หรือที่ปรึกษาด้านอื่น ๆ
- (4) ผู้ให้บริการใด ๆ หรือตัวแทนผู้ให้บริการ (รวมไปถึงผู้ให้บริการช่วง) ของบริษัท บริษัท เช่น บริการเกี่ยวกับการชำระเงิน บริการด้านเทคโนโลยี บริการคลาวด์ บริการจัดหาผู้รับจ้าง ปฏิบัติงาน บริการจัดเก็บสิ่งของ และการดำเนินการเกี่ยวกับเอกสาร บริการเก็บบันทึกข้อมูล

บริการสแกนเอกสาร บริการรับส่งไปรษณีย์ บริการจัดพิมพ์ บริการส่งพัสดุหรือบริการรับส่งพัสดุโดยพนักงานรับส่งพัสดุ บริการวิเคราะห์ข้อมูล บริการทำการตลาด บริการทำการวิจัยหรือบริการอื่น ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท

- (5) องค์กรที่เกี่ยวข้องกับการประกันภัย เช่น สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยสมาคมประกันวินาศภัยไทย หรือสภาอุตสาหกรรมแห่งประเทศไทย
- (6) หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย คณะกรรมการต่าง ๆ ที่จัดตั้งขึ้นตามกฎหมาย หน่วยงานรัฐหรือหน่วยงานกำกับดูแล หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือบุคคลอื่นใดในประเทศที่บริษัท หรือบริษัทในกลุ่มบริษัทต้องเปิดเผยข้อมูลให้ (ก) ตามหน้าที่ตามกฎหมาย และ/หรือตามหน้าที่ในการปฏิบัติตามกฎระเบียบในประเทศไทย และอาจรวมถึงหน่วยงานของรัฐในประเทศที่กลุ่มบริษัทตั้งอยู่ หรือ (ข) ตามข้อตกลง หรือนโยบายระหว่างบริษัทในกลุ่มบริษัท กับรัฐ หน่วยงานกำกับดูแล หรือบุคคลอื่น ๆ ที่เกี่ยวข้อง
- (7) ผู้เข้าทำธุรกรรม หรือจะเข้าทำธุรกรรมกับบริษัทโดยข้อมูลส่วนบุคคลของท่านอาจเป็นส่วนหนึ่งของการซื้อหรือขาย หรือเป็นส่วนหนึ่งของการเสนอซื้อหรือเสนอขายของกิจการของบริษัท (หากมี)
- (8) บุคคลอื่นใดที่ท่านได้ให้ความยินยอมโดยชัดแจ้ง เพื่อให้บรรลุเป้าหมายตามวัตถุประสงค์ที่กล่าวมาแล้วข้างต้น

[โปรดระบุบุคคลที่ท่านอาจได้รับข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

6. การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัท หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่ในประเทศไทยหรือนอกประเทศไทย ทั้งนี้ ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท เราจะดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัทที่ได้รับการอนุมัติจากคณะกรรมการ (หากมี)

7. การเก็บรักษาข้อมูลส่วนบุคคล

เราอาจเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ นานเท่าที่จำเป็นต้องเก็บเพื่อการดำเนินการให้บรรลุตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของท่านตามที่ระบุข้างต้น ทั้งนี้บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไม่เกิน 10 ปี นับแต่วันที่ท่านสิ้นสุดความสัมพันธ์ หรือการติดต่อครั้งสุดท้ายกับเรา บริษัทอาจเก็บรักษาข้อมูลส่วนบุคคลของท่านนานกว่าที่กำหนดหากกฎหมายอนุญาต

เราจะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อทำการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่ไม่สามารถระบุตัวท่าน ตามระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลข้างต้น

8. การใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม

บริษัทมีสิทธิในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านที่บริษัทได้เก็บรวบรวมไว้ก่อนวันที่พรบ.คุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลมีผลใช้บังคับต่อไปตามวัตถุประสงค์เดิม หากท่านไม่ประสงค์ที่จะให้บริษัทเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวต่อไป ท่านสามารถแจ้งบริษัทเพื่อขอถอนความยินยอมของท่านตามหลักเกณฑ์ที่กฎหมายกำหนดได้ที่ [โปรดระบุช่องทางการขอถอนความยินยอม]

9. การรักษาความปลอดภัย

บริษัทมีการใช้มาตรการรักษาความปลอดภัยภายในบริษัทและการใช้บังคับนโยบายอย่างเข้มงวดในการเก็บรักษาข้อมูลส่วนบุคคลของท่านให้ปลอดภัย ซึ่งรวมถึงการเข้ารหัสข้อมูล และมาตรการป้องกันการเข้าถึงข้อมูล โดยบริษัทกำหนดให้บุคลากรของบริษัทและผู้รับจ้างภายนอกจะต้องปฏิบัติตามมาตรฐานและนโยบายความเป็นส่วนบุคคลที่เหมาะสม รวมถึงจะต้องจัดให้มีการดูแลรักษาข้อมูลและมีมาตรการที่เหมาะสมในการใช้หรือการส่งหรือโอนข้อมูลส่วนบุคคลของท่าน

10. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

- (1) เพิกถอน หรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านที่ได้ให้ไว้กับเรา
- (2) ขอเข้าถึง ขอรับสำเนา หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เกี่ยวกับท่านโดยท่านไม่ได้ให้ความยินยอม

(3) ขอรับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับท่าน หรือขอให้ส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น

(4) คัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

(ก.) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เนื่องจากเป็นการจำเป็นเพื่อประโยชน์สาธารณะ หรือการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย ตามมาตรา 24 (4) หรือ (5) แห่งพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เว้นแต่เราสามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(ข.) การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

(ค.) การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะของเรา

(5) ขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามหลักเกณฑ์ที่กฎหมายกำหนด

(6) ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านตามหลักเกณฑ์ที่กฎหมายกำหนด

(7) ขอให้แก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด หากเราไม่สามารถดำเนินการให้ได้ ท่านมีสิทธิขอบันทึกคำร้องขอของท่านพร้อมเหตุผลในการดำเนินการได้ตามหลักเกณฑ์ที่กฎหมายกำหนด

ทั้งนี้ เราขอสงวนสิทธิ์ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและตามหลักเกณฑ์ที่กฎหมายกำหนด อย่างไรก็ตาม เราอาจเรียกเก็บค่าใช้จ่ายตามสมควรเพื่อดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้นด้วย

นอกจากสิทธิของท่านตามที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของบริษัทต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

11. การแก้ไขเปลี่ยนแปลงนโยบายฉบับนี้

บริษัทขอสงวนสิทธิในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฉบับนี้ บริษัทจะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายให้ท่านทราบ และ/หรือจะขอความยินยอมจากท่าน (หากกฎหมายกำหนดให้ต้องได้รับความยินยอม)

12. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายความเป็นส่วนตัวฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเราที่

รายละเอียดของบริษัท

ชื่อ: [ชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับเรื่องขอใช้สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท [ระบุชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับ
เรื่องขอใช้สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

11.3 ตัวอย่างร่างข้อความแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลสำหรับพนักงาน

Version: [ระบุVersion หรือวันที่อ้างอิงของนโยบาย]

นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับพนักงาน

[ชื่อบริษัท]

[ชื่อบริษัท] (“บริษัท”) และบริษัทในเครือหรือบริษัทในกลุ่มบริษัท [ชื่อบริษัท] (“กลุ่มบริษัท”) (เรียกรวมกันว่า “เรา” “พวกเรา” “ของเรา”) ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของเราเกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลของท่าน บริษัทจึงได้จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (“นโยบาย”) ฉบับนี้ขึ้นเพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”)

1. บทนิยาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายถึง ข้อมูลตามที่กำหนดไว้ในมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่อาศัยอำนาจ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลในการตราขึ้น และตามที่มีการแก้ไขเป็นครั้งคราว

“คณะกรรมการ” หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2. ข้อมูลส่วนบุคคลที่บริษัทอาจทำการเก็บรวบรวม

2.1 กรณีที่ท่านเป็นผู้สมัครงาน

- (1) **ข้อมูลที่ใช้ระบุตัวบุคคล** เช่น ชื่อ ที่อยู่ หรือรายละเอียดของสถานที่ติดต่ออื่น เพศ อายุ สัญชาติ สถานภาพการสมรส วันเดือนปีเกิด รายละเอียดบัญชีธนาคาร เลขที่หนังสือเดินทาง/ บัตรประจำตัวประชาชน ข้อมูลเกี่ยวกับผู้ที่อยู่ในการดูแลของท่าน และภาพถ่าย เป็นต้น
- (2) **ข้อมูลเกี่ยวกับคุณวุฒิและประวัติการทำงานของท่าน** เช่น ประกาศนียบัตรจากโรงเรียน/ มหาวิทยาลัย ประวัติการเรียน การทดสอบทางวิชาการหรือภาษา ใบอนุญาตประกอบอาชีพ หรือวิชาชีพ (เช่น ใบอนุญาตตัวแทน/นายหน้าประกันวินาศภัย) หนังสือรับรองและหนังสืออ้างอิง
- (3) **ข้อมูลส่วนบุคคลที่มีความอ่อนไหว** เช่น ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น โดย บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเหล่านี้ต่อเมื่อท่านได้ผ่านการสัมภาษณ์งานแล้ว โดยบริษัทจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเหล่านี้เพื่อพิจารณาประกอบการเข้าทำสัญญา และประเมินความพร้อมในการเข้าทำงานของท่าน [หมายเหตุ: ขึ้นอยู่กับแต่ละบริษัท และขึ้นอยู่กับความจำเป็นในการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว]
- (4) **ข้อมูลส่วนบุคคลของบุคคลที่เกี่ยวข้อง** เช่น ข้อมูลบุคคลอ้างอิง และบุคคลที่ติดต่อได้ เป็นต้น

2.2 กรณีที่ท่านเป็นพนักงาน

หากท่านได้รับพิจารณาและเข้าทำสัญญาเป็นพนักงานของบริษัท บริษัทจะเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคลของท่านที่ไว้ตั้งแต่ขั้นตอนการสมัครงาน และจะเก็บรวบรวมข้อมูลส่วนบุคคลอื่น ๆ ของท่านเพิ่มเติม ดังนี้

- (1) **รายละเอียดการทำงานพื้นฐาน** เช่น หมายเลขพนักงาน ตำแหน่งงาน รายละเอียดของงาน สายการบังคับบัญชา ชั่วโมงการทำงาน ระเบียบและเงื่อนไขของการจ้างงาน เป็นต้น
- (2) **ข้อมูลทั่วไปที่เก็บรวบรวมจากการปฏิบัติงาน** เช่น ประวัติส่วนตัว ประวัติการเกณฑ์ทหาร ข้อมูลการสัมภาษณ์งาน และหลักฐานอ้างอิงต่าง ๆ ข้อมูลจากระบบเฝ้าระวังและควบคุมการเข้า-ออกอาคารและสถานที่ กล้องวงจรปิด เทปบันทึกและการบันทึกข้อมูลการใช้โทรศัพท์

อีเมล และการบันทึกข้อมูลการใช้อินเทอร์เน็ตที่มีความเกี่ยวข้องกับการทำงานของท่านกับบริษัท เท่าที่ไม่ขัดกับกฎหมาย

- (3) **ข้อมูลเกี่ยวกับผลประโยชน์และค่าจ้าง** เช่น รายละเอียดการจ่ายเงินเดือนและผลประโยชน์อื่นของท่าน ประกันสังคม ข้อมูลเกี่ยวกับการเกษียณอายุ/บำนาญ กองทุนสำรองเลี้ยงชีพ ข้อมูลทางภาษี และข้อมูลของบุคคลภายนอกผู้ได้รับผลประโยชน์
- (4) **ประวัติเกี่ยวกับประสิทธิภาพของการทำงาน** รวมถึง การประเมิน ผลตอบรับ ข้อมูลเกี่ยวกับระเบียบข้อบังคับการทำงานหรือการร้องทุกข์ ประวัติวันหยุดประจำปี ประวัติการลาป่วยหรือขาดงาน หรือข้อมูลที่เกี่ยวข้องกับการทำงานในสถานประกอบการและความปลอดภัย รวมถึงการตรวจสอบและการประเมินความเสี่ยง
- (5) **ข้อมูลส่วนบุคคลที่มีความอ่อนไหว** เช่น ประวัติสุขภาพ ทั้งนี้เป็นไปเพื่อการให้สวัสดิการแก่ท่าน เช่น การทำประกันภัยสุขภาพ หรือการเบิกจ่ายค่ารักษาพยาบาล

[โปรดระบุข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมให้ครบถ้วน]

ในกรณีที่บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อการเข้าทำสัญญา การประเมินความสามารถในการทำงาน การบริหารจัดการสวัสดิการ การปฏิบัติตามสัญญา หรือการปฏิบัติหน้าที่ตามกฎหมาย หากท่านไม่ให้ข้อมูลส่วนบุคคลที่จำเป็นต่อการดำเนินงานของบริษัท บริษัทอาจไม่สามารถดำเนินการตามวัตถุประสงค์ที่ระบุไว้ในนโยบายฉบับนี้หรือให้บริการแก่ท่านได้อย่างเต็มรูปแบบ หรือท่านอาจไม่สามารถใช้บริการของบริษัทได้อย่างเหมาะสม หรืออาจส่งผลกระทบต่อการใช้บริการตามกฎหมายใด ๆ ที่บริษัทหรือท่านมีหน้าที่ต้องปฏิบัติตาม

เมื่อท่านให้ข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับบุคคลภายนอกแก่เรา (ซึ่งบุคคลภายนอกดังกล่าวรวมถึงแต่ไม่จำกัดเพียงผู้เอาประกันภัย สมาชิกในครอบครัว ญาติ หรือบุคคลอ้างอิง) ท่านต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขอความยินยอมหรือแจ้งนโยบายฉบับนี้แก่บุคคลที่สามในนามของบริษัท ทั้งนี้ ท่านรับรองและรับประกันความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมทั้งรับรองและรับประกันว่าท่านได้แจ้งให้บุคคลเหล่านั้นทราบอย่างครบถ้วนแล้วเกี่ยวกับรายละเอียดตามนโยบายฉบับนี้

3. เราเก็บรวบรวมข้อมูลส่วนบุคคลของท่านอย่างไร

โดยทั่วไป บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยตรงจากท่าน และในบางกรณีบริษัทอาจจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านจากแหล่งอื่น หรือบุคคลอื่น เช่น บุคคลที่แนะนำท่าน ให้เรา บริษัทจัดหางาน โรงพยาบาล หน่วยงานของรัฐที่เกี่ยวข้อง หรือบุคคลอื่น ๆ แล้วแต่กรณี

[โปรดระบุแหล่งที่มาของการเก็บรวบรวมข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

4.1 สำหรับผู้สมัครงาน

- (1) เพื่อพิจารณาและดำเนินกระบวนการต่าง ๆ ที่จำเป็นในการรับสมัครงาน เช่น การพิจารณาประวัติของท่าน การสัมภาษณ์งาน การเตรียมเอกสารประกอบการรับสมัครงาน การประเมินความสามารถในการทำงาน การจัดการเกี่ยวกับการตรวจสอบสุขภาพ และการดำเนินการอื่น ๆ ที่เกี่ยวข้อง

4.2 สำหรับพนักงาน

- (1) เพื่อดำเนินการเกี่ยวกับการเข้าทำสัญญา หรือการดำเนินการตามสัญญา เช่น เพื่อการพิจารณาข้อตกลงเกี่ยวกับการจ้าง การเตรียมเอกสารเพื่อเข้าทำสัญญาจ้าง การเข้าทำสัญญาจ้างกับบริษัท รวมถึงการปฏิบัติตามสิทธิและหน้าที่ตามสัญญาจ้างระหว่างท่านกับบริษัท
- (2) เพื่อบริหารจัดการการทำงานและสวัสดิการให้แก่ท่านและ/หรือบุคคลภายนอก (หากมี) เช่น การประเมินความสามารถในการทำงาน การวัด/ ประเมินผล การวิเคราะห์และจัดอบรม เพื่อพัฒนาศักยภาพและความสามารถในการทำงานของท่าน การบริหารจัดการทรัพยากรบุคคลของเรา การตรวจสอบข้อมูลของท่านตามกฎหมาย การช่วยเหลือพนักงานในการปรับตัวเข้ากับงานใหม่ การจัดสวัสดิการ จัดทำบันทึกข้อมูลลูกจ้าง การทำประกันภัย ประวัติทางการแพทย์และแผนประกัน การวางแผนและการดำเนินการเกี่ยวกับการจ้างพนักงานและการฝึกอบรม การเลื่อนขั้น การย้ายงาน การมอบหมายให้พนักงานไปปฏิบัติงานที่อื่น และเพื่อปฏิบัติตามกระบวนการ กฎหมายและกฎเกณฑ์ที่ใช้บังคับ รวมถึงการวางแผนกำลังคน ข้อกำหนดการจ่ายค่าจ้าง ค่าชดเชย ผลประโยชน์ แผนค่าตอบแทน ข้อเสนอในอนาคต รางวัล บัญชีค่าตอบแทน การประเมินผลการปฏิบัติงาน การรายงานภายใน การวิเคราะห์

ข้อมูล และการจัดการงานในการจ้างงานรายเดือนหรือรายวัน การติดต่อสื่อสารภายใน การแจ้งการนัดหมายแก่บุคคลทั้งภายในและภายนอก การประเมินใบสมัครงานสำหรับโอกาสในงานใหม่และการตัดสินใจในการจ้างงาน รวมถึงการประเมินการเลื่อนตำแหน่ง ความสามารถในการทำงานของท่าน การตรวจสอบโอกาสที่เท่าเทียมกัน

(3) **เพื่อการทำวิจัย การวิเคราะห์ข้อมูล และการทำวิจัยสถิติ**เกี่ยวกับการจ้างงาน การวัด/ประเมินผล หรือกระบวนการที่คล้ายคลึงที่เกี่ยวกับการจ้างงานและบริหารจัดการทรัพยากรบุคคลของเรา ซึ่งรวมไปถึงการทำแบบสำรวจ สถิติของรัฐบาล หรือการตอบแบบฟอร์มคำร้องใด ๆ ของรัฐ

(4) **เพื่อดำเนินการตามความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท** กล่าวคือ

(ก) เพื่อการดำเนินการให้เป็นไปตามข้อกำหนดภายใต้นโยบายภายในของเราที่ยึดถือปฏิบัติ

(ข) เพื่อวัตถุประสงค์ในการบริหารจัดการ จัดเก็บ บันทึก สำรอง หรือทำลายข้อมูลส่วนบุคคล

(ค) เพื่อการติดตามพฤติกรรมของท่าน รวมถึงการตรวจสอบและสืบสวนข้อร้องเรียนเกี่ยวกับความประพฤติที่ไม่เหมาะสม การกระทำความผิดทางวินัย และ/หรือกฎหมาย ไม่ว่าจะเป็นกระบวนการสืบสวนภายใน หรือการให้ความร่วมมือกับหน่วยงานรัฐที่มีอำนาจ

(ง) เพื่อจัดระบบรักษาความปลอดภัยให้แก่ท่าน พนักงานคนอื่น หรือบุคคลอื่น ๆ ที่เข้าออกบริเวณอาคารของบริษัท

(จ) เพื่อวัตถุประสงค์ในการปรับโครงสร้างองค์กรของบริษัท และเพื่อการทำธุรกรรมของบริษัท

(ฉ) เพื่อการเข้าซื้อหรืออาจจำหน่ายหนึ่ง หรือมากกว่าหนึ่งธุรกิจ (บางส่วนของธุรกิจ) ของเรา

(5) **เพื่อการปฏิบัติตามกฎหมายและการตรวจสอบธุรกิจของเรา** ไม่ว่าจะเป็นการตรวจสอบภายใน หรือการตรวจสอบจากบุคคลภายนอก เพื่อดำเนินการให้เป็นไปตามข้อกำหนดของ

กฎหมาย กฎ ระเบียบ ข้อตกลง หรือนโยบายที่ใช้บังคับ ซึ่งกำหนดขึ้นโดยหน่วยงานกำกับดูแลของรัฐ หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย หน่วยงานรัฐ หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือหน่วยงานที่ดูแลธุรกิจประกันภัย ไม่ว่าหน่วยงานใดก็ตาม รวมถึงเพื่อวัตถุประสงค์ของการบังคับใช้กฎหมาย หรือการให้ความช่วยเหลือ ให้ความร่วมมือ การสืบสวนโดยเรา หรือในนามของเรา โดยเจ้าหน้าที่ตำรวจ หรือโดยหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศ และการดำเนินการตามหน้าที่ในการรายงาน และข้อกำหนดต่าง ๆ ตามที่กฎหมายกำหนด หรือตามที่มีการตกลงเห็นชอบกับหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศหรือเขตการปกครองใด ๆ หรือการดำเนินการตามคำสั่งโดยชอบด้วยกฎหมายของพนักงานเจ้าหน้าที่ หรือหน่วยงานของรัฐ

(6) เพื่อการดำเนินการอื่น ๆ ที่จำเป็น ซึ่งเกี่ยวข้องโดยตรงกับวัตถุประสงค์ใด ๆ ข้างต้น

เว้นแต่กฎหมายและกฎระเบียบที่ใช้บังคับ รวมถึง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลจะอนุญาตให้กระทำเป็นอย่างอื่น เราจะแจ้งและขอความยินยอมจากท่าน หากเราประสงค์จะใช้ข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์อื่นใดนอกเหนือไปจากที่ระบุไว้ในนโยบายความเป็นส่วนตัวฉบับนี้ หรือนอกเหนือไปจากวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับนโยบายความเป็นส่วนตัวนี้

[โปรดระบุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

5. การเปิดเผยข้อมูลส่วนบุคคลของท่าน

ในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ข้างต้น บริษัทอาจจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลภายนอก ดังนี้

- (1) บริษัทในเครือ
- (2) ที่ปรึกษาภายในหรือภายนอก ผู้เชี่ยวชาญ หรือที่ปรึกษาอื่นใดของบริษัทในเครือ เช่น หน่วยงาน ผู้ตรวจสอบบัญชี หรือที่ปรึกษาด้านอื่น ๆ
- (3) ผู้ให้บริการใด ๆ ซึ่งเป็นคู่สัญญาฝ่ายที่สาม หรือตัวแทนผู้ให้บริการใด ๆ ที่จำเป็นในการดำเนินการตามวัตถุประสงค์ในการประมวลผลข้างต้น เช่น ตัวแทน/นายหน้าประกันวินาศภัย บริษัทผู้รับประกันภัย ผู้สรรหาบุคลากร ผู้ให้บริการสนับสนุน และ/หรือดูแลรักษาระบบ

เทคโนโลยีสารสนเทศของบริษัท หรือโปรแกรมที่ช่วยในการสรรหาบุคลากร ระบบบัญชี ค่าตอบแทน ผลประโยชน์ และระบบของฝ่ายทรัพยากรบุคคลอื่น ๆ

- (4) หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย คณะกรรมการต่าง ๆ ที่จัดตั้งขึ้นตามกฎหมาย หน่วยงานรัฐหรือหน่วยงานกำกับดูแล หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือบุคคลอื่นใดในประเทศที่บริษัท หรือบริษัทในกลุ่มบริษัทต้องเปิดเผยข้อมูลให้ (ก) ตามหน้าที่ตามกฎหมาย และ/ หรือตามหน้าที่ในการปฏิบัติตามกฎระเบียบในประเทศไทย และอาจรวมถึงหน่วยงานของรัฐในประเทศที่กลุ่มบริษัทตั้งอยู่ หรือ(ข) ตามข้อตกลง หรือนโยบายระหว่างบริษัทในกลุ่มบริษัท กับรัฐ หน่วยงานกำกับดูแล หรือบุคคลอื่น ๆ ที่เกี่ยวข้อง
- (5) ผู้เข้าทำธุรกรรม หรือจะเข้าทำธุรกรรมกับบริษัทโดยข้อมูลส่วนบุคคลของท่านอาจเป็นส่วนหนึ่งของการซื้อหรือขาย หรือเป็นส่วนหนึ่งของการเสนอซื้อหรือเสนอขายของกิจการของบริษัท (หากมี)
- (6) บุคคลอื่นใดที่ท่านได้ให้ความยินยอมโดยชัดแจ้งให้เปิดเผยข้อมูลส่วนบุคคลของท่านต่อบุคคลหรือหน่วยงานนั้น ๆ ได้
- (7) กองทุนสำรองเลี้ยงชีพ เพื่อให้บรรลุเป้าหมายตามวัตถุประสงค์ที่กล่าวมาแล้วข้างต้น

[โปรดระบุบุคคลที่ท่านอาจได้รับข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วน]

6. การโอนข้อมูลไปยังต่างประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัท หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่นอกประเทศไทย ทั้งนี้ ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท เราจะดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัทที่ได้รับการอนุมัติจากคณะกรรมการ (หากมี)

7. การเก็บรักษาข้อมูลส่วนบุคคล

บริษัทมีนโยบายที่จะเก็บรักษาข้อมูลส่วนบุคคลตราบเท่าที่จำเป็น เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดข้างต้น โดยบริษัทมีนโยบายเก็บรักษาข้อมูลส่วนบุคคลของท่านตลอดระยะเวลาการจ้างงาน หรือตลอดระยะเวลาที่มีนิติสัมพันธ์ต่อกัน และเมื่อสิ้นสุดนิติสัมพันธ์ต่อกันแล้ว บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านต่อไปอีกเป็นระยะเวลา 10 ปี เว้นแต่กฎหมายที่ใช้บังคับกำหนดหรืออนุญาต สำหรับการเก็บรักษาในระยะเวลาที่ยาวกว่าที่ระบุข้างต้น

8. การใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม

บริษัทมีสิทธิในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านที่บริษัทได้เก็บรวบรวมไว้ก่อนวันที่พรบ.คุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลมีผลใช้บังคับต่อไปตามวัตถุประสงค์เดิม หากท่านไม่ประสงค์ที่จะให้บริษัทเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวต่อไป ท่านสามารถแจ้งบริษัทเพื่อขอถอนความยินยอมของท่านตามหลักเกณฑ์ที่กฎหมายกำหนดได้ที่ [โปรดระบุช่องทางการขอถอนความยินยอม]

9. การรักษาความปลอดภัย

บริษัทมีการใช้มาตรการรักษาความปลอดภัยภายในบริษัทและการใช้บังคับนโยบายอย่างเข้มงวดในการเก็บรักษาข้อมูลส่วนบุคคลของท่านให้ปลอดภัย ซึ่งรวมถึงการเข้ารหัสข้อมูล และมาตรการป้องกันการเข้าถึงข้อมูล โดยบริษัทกำหนดให้บุคลากรของบริษัทและผู้รับจ้างภายนอกจะต้องปฏิบัติตามมาตรฐานและนโยบายความเป็นส่วนตัวส่วนบุคคลที่เหมาะสม รวมถึงจะต้องจัดให้มีการดูแลรักษาข้อมูลและมีมาตรการที่เหมาะสมในการใช้หรือการส่งหรือโอนข้อมูลส่วนบุคคลของท่าน

10. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

- (1) เพิกถอน หรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านที่ได้ให้ไว้กับเรา
- (2) ขอเข้าถึง ขอรับสำเนา หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เกี่ยวกับท่านโดยท่านไม่ได้ให้ความยินยอม

(3) ขอรับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับท่าน หรือขอให้ส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น

(4) คัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

(ก.) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เนื่องจากเป็นการจำเป็นเพื่อประโยชน์สาธารณะ หรือการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย ตามมาตรา 24 (4) หรือ (5) แห่งพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เว้นแต่เราสามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(ข.) การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

(ค.) การประมวลผลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะของเรา

(5) ขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามหลักเกณฑ์ที่กฎหมายกำหนด

(6) ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านตามหลักเกณฑ์ที่กฎหมายกำหนด

(7) ขอให้แก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด หากเราไม่สามารถดำเนินการให้ได้ ท่านมีสิทธิขอบันทึกคำร้องขอของท่านพร้อมเหตุผลในการดำเนินการได้ตามหลักเกณฑ์ที่กฎหมายกำหนด

ทั้งนี้ เราขอสงวนสิทธิ์ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและตามหลักเกณฑ์ที่กฎหมายกำหนด อย่างไรก็ตาม เราอาจเรียกเก็บค่าใช้จ่ายตามสมควรเพื่อดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้นด้วย

นอกจากสิทธิของท่านตามที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของบริษัทต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

11. การแก้ไขเปลี่ยนแปลงนโยบายฉบับนี้

บริษัทขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฉบับนี้ บริษัทจะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายให้ท่านทราบ และ/หรือจะขอความยินยอมจากท่าน (หากกฎหมายกำหนดให้ต้องได้รับความยินยอม)

12. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายความเป็นส่วนตัวฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเราที่

รายละเอียดของบริษัท

ชื่อ: [ชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับเรื่องขอใช้สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

รายละเอียดเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท [ระบุชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [หมายเลขโทรศัพท์และเวลาทำการ]

[อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม] [แนะนำให้แยกระหว่าง อีเมลรับเรื่องขอใช้
สิทธิ กับ อีเมลรับเรื่องสอบถามข้อมูลเพิ่มเติม]

[ช่องทางอื่น ๆ (ถ้ามี)]

11.4 ตัวอย่างแบบความยินยอมสำหรับการดำเนินกิจกรรมทางการตลาด

Version [ระบุ Version หรือวันที่อ้างอิง]

แบบความยินยอม

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการเสนอผลิตภัณฑ์

เพื่อเป็นการให้ข้อมูลแก่ท่านเกี่ยวกับผลิตภัณฑ์และบริการของ[ชื่อบริษัท] (“บริษัท”) และบริษัทในเครือหรือบริษัทในกลุ่มบริษัท [ชื่อบริษัท] (“กลุ่มบริษัท”) (เรียกรวมกันว่า “เรา” “พวกเรา” “ของเรา”) บริษัทจำเป็นต้องใช้ข้อมูลส่วนบุคคลของท่าน ได้แก่ ชื่อ นามสกุล อายุ เพศ ที่อยู่ อีเมล ที่อยู่ หมายเลขโทรศัพท์ และข้อมูลส่วนบุคคลอื่นใด ดังระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคลของเรา [แทรกลิงก์นโยบายคุ้มครองข้อมูลส่วนบุคคล หากเป็นการขอความยินยอมทางอิเล็กทรอนิกส์] เพื่อใช้ในการดำเนินการส่งเนื้อหาเกี่ยวกับการส่งเสริมการขาย และการสื่อสารการตลาดทางตรงเกี่ยวกับผลิตภัณฑ์และบริการของเรา คำแนะนำและข้อมูลในเรื่องต่าง ๆ ซึ่งรวมถึงการประกันภัย โปรแกรมให้รางวัล การให้ผลประโยชน์สำหรับการเป็นลูกค้าที่มีความภักดีต่อแบรนด์ การให้สิทธิพิเศษ กิจกรรมการกุศล กิจกรรมที่ไม่หวังผลกำไร และการจัดกิจกรรมทางการตลาด การประกวด จับฉลากชิงโชค งานอีเว้นท์ และการแข่งขันต่าง ๆ ที่ท่านอาจสนใจ โดยเราอาจต้องเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคลากร และคู่ค้าของเราซึ่งเกี่ยวข้องกับการดำเนินกิจกรรมทางการตลาด และการกิจกรรมอื่น ๆ ที่เกี่ยวข้อง เพื่อที่บริษัท และบุคคลดังกล่าวสามารถดำเนินการจัดกิจกรรมทางการตลาด และมอบสิทธิพิเศษต่าง ๆ แก่ท่านได้

ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลของท่านจะเป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัท [ตามแนบ หรือตามลิงก์]

หากท่านไม่ต้องการรับการสื่อสาร หรือข่าวสาร รวมทั้งสิทธิประโยชน์ใด ๆ เกี่ยวกับผลิตภัณฑ์หรือบริการของเรา ท่านอาจขอเพิกถอนความยินยอมไม่ว่าในเวลาใดก็ตาม (แจ้งผลกระทบในกรณีเพิกถอนความยินยอม) โดยติดต่อมาที่บริษัทตามรายละเอียดด้านล่าง หรือ Unsubscribe จากข้อความทางอีเมล หรือ SMS

[ระบุชื่อบริษัท]

ที่อยู่: [ที่อยู่สำนักงานใหญ่บริษัท]

ช่องทางการติดต่อ: [เบอร์โทรศัพท์ หรืออีเมล และเวลาทำการ]

การที่ท่าน [คลิก] หรือ[ลงลายมือชื่อ] ด้านล่างนี้ เป็นการที่ท่านรับทราบและให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อให้บริษัทดำเนินการตามที่ระบุในแบบความยินยอมนี้

ลงชื่อ _____

วันที่

11.5 ตัวอย่างร่างข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคล

ข้อตกลงเพิ่มเติม¹⁰⁸

สัญญาการประมวลผลข้อมูลส่วนบุคคล

ข้อตกลงเพิ่มเติมหรือสัญญาการประมวลผลข้อมูลส่วนบุคคลฉบับนี้ (“ข้อตกลงเพิ่มเติม”) ลงวันที่ [วัน/ เดือน/ ปี] (“วันที่ตกลงให้มีผลใช้บังคับ”) ได้จัดทำขึ้นระหว่าง

[ชื่อบริษัท] ซึ่งเป็นนิติบุคคลที่จัดตั้งภายใต้กฎหมายไทย มีสำนักงานตั้งอยู่ที่ [ระบุรายละเอียด] (“บริษัท” หรือ “ผู้ควบคุมข้อมูลส่วนบุคคล”) ฝ่ายหนึ่ง

กับ

กรณีที่ 1: ผู้ให้บริการเป็นนิติบุคคล

[ระบุชื่อบริษัทผู้ให้บริการ] ซึ่งเป็นนิติบุคคลที่จัดตั้งภายใต้กฎหมายของ [ระบุรายละเอียด] มีสำนักงานตั้งอยู่ที่ [ระบุรายละเอียด] (“ผู้ให้บริการ” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล”) อีกฝ่ายหนึ่ง

หรือ

กรณีที่ 2: ให้บริการเป็นบุคคลธรรมดา (เช่น ตัวแทนหรือนายหน้าประกันวินาศภัย)

[ระบุชื่อผู้ให้บริการ] ซึ่งเป็นผู้ถือบัตรประจำตัวประชาชน/ หนังสือเดินทางหมายเลข [ระบุรายละเอียด] และ/ หรือผู้ถือใบอนุญาตตัวแทน/ นายหน้าประกันวินาศภัยตามกฎหมายเลขที่ [ระบุรายละเอียด] อยู่ที่ [ระบุรายละเอียด] (“ผู้ให้บริการ” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล”) อีกฝ่ายหนึ่ง

โดยที่:

¹⁰⁸ สามารถนำบันทึกข้อตกลงนี้ไปใช้แนบท้ายสัญญาที่มีอยู่แล้วระหว่างบริษัทกับผู้ให้บริการ

- บริษัทและผู้ให้บริการ ในข้อตกลงเพิ่มเติมนี้ ต่อไปจะเรียกแต่ละฝ่ายว่า “คู่สัญญาฝ่ายหนึ่ง” และเรียกรวมกันว่า “คู่สัญญาทั้งสองฝ่าย”
- คู่สัญญาทั้งสองฝ่ายตกลงให้ข้อตกลงเพิ่มเติมนี้ มีผลนับตั้งแต่วันที่ตกลงให้มีผลใช้บังคับและให้มีผลต่อไปจนกว่าสัญญาที่มีอยู่จะสิ้นสุด
- บริษัทและผู้ให้บริการได้เข้าทำสัญญา [ชื่อสัญญา เช่นสัญญาซื้อขาย สัญญาบริการ] ลงวันที่ [ระบุวันที่] ทั้งนี้กรณีคู่สัญญาทั้งสองฝ่ายได้เข้าทำสัญญาร่วมกันไว้มากกว่าหนึ่งฉบับ (โปรดดูเอกสารแนบท้าย 1) เพื่อมิให้เป็นที่ยสงสัย ให้สัญญาในที่นี้หมายความว่ารวมถึงสัญญาใด ๆ ที่บริษัทได้เข้าทำกับผู้ให้บริการที่ไม่ได้ระบุอยู่ในเอกสารแนบท้าย 1 แต่ยังมีผลใช้บังคับอยู่ในวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) (เรียกว่า “สัญญาที่มีอยู่”)
- คู่สัญญาทั้งสองฝ่ายรับทราบ ว่า ผู้ให้บริการอาจเข้าถึง ได้รับ และ/ หรือเก็บรวบรวม ใช้ เปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลในนามของบริษัทเพื่อการให้บริการเพื่อให้เป็นไปตามสัญญาที่มีอยู่
- ข้อตกลงเพิ่มเติมนี้ได้ระบุสิทธิและหน้าที่ของคู่สัญญาทั้งสองฝ่าย รวมถึงพนักงาน และบุคคลภายนอก ซึ่งกระทำการแทนในนามผู้ให้บริการ และยังใช้กับข้อมูลส่วนบุคคลที่โอนหรือเข้าถึงได้ระหว่างคู่สัญญาทั้งสองฝ่ายอันเนื่องมาจากการให้บริการดังกล่าวด้วย
- ในข้อตกลงเพิ่มเติมนี้ อาจจะมีการอ้างถึงคำว่า “ข้อมูลส่วนบุคคลทั่วไป” และ “ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” แต่ถ้าหากไม่มีการอ้างถึงโดยเฉพาะเจาะจง ให้ถือว่าหมายถึง “ข้อมูลส่วนบุคคล”
- คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อตกลงเพิ่มเติมนี้เป็นส่วนที่เพิ่มเติมและเป็นส่วนหนึ่งของสัญญาที่มีอยู่ และหากข้อตกลงเพิ่มเติมนี้มีเนื้อหาหรือข้อความใดที่ขัดแย้งกับสัญญาที่มีอยู่ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้เนื้อหาหรือข้อความดังกล่าวของข้อตกลงเพิ่มเติมมีผลใช้บังคับ

ดังนั้น คู่สัญญาทั้งสองฝ่ายจึงตกลงกันดังนี้

1. คำรับรองของคู่สัญญา

- 1.1 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เปิดเผยแก่หรือให้ผู้ให้บริการเข้าถึงข้อมูลส่วนบุคคลเพื่อบรรลุวัตถุประสงค์ในการดำเนินการตามคำสั่งหรือในนามของบริษัทเท่านั้น โดยที่ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตกลงที่จะดำเนินการภายใต้คำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลตามที่กำหนดในสัญญาที่มีอยู่ และในข้อตกลงเพิ่มเติมเท่านั้น
- 1.2 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า รายละเอียดการประมวลผลข้อมูลส่วนบุคคลระบุอยู่ในเอกสารแนบท้าย 2 โดยที่การประมวลผลข้อมูลส่วนบุคคลอื่นที่ผู้ให้บริการกระทำนอกเหนือจากที่ระบุไว้ในเอกสารแนบท้าย 2 หรือนอกเหนือจากคำสั่งเป็นหนังสือตามที่ได้ตกลงไว้กับบริษัท ถือว่าเป็นการกระทำหรือการประมวลผลข้อมูลส่วนบุคคลของผู้ให้บริการโดยลำพัง ไม่เกี่ยวข้องกับบริษัทในทางใด ๆ และผู้ให้บริการจะรับผิดชอบเกี่ยวกับการดำเนินการดังกล่าวผู้เดียวเท่านั้น
- 1.3 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า รายละเอียดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลระบุอยู่ในเอกสารแนบท้าย 3 โดย ณ วันที่ตกลงให้มีผลบังคับใช้ของข้อตกลงเพิ่มเติมนี้ ผู้ให้บริการรับรองว่า ผู้ให้บริการมีมาตรการข้างต้นตามที่ได้ระบุอยู่ในเอกสารแนบท้าย 3 แล้ว และจะจัดให้มีการดูแลรักษามาตรการดังกล่าวเป็นครั้งคราว ตามที่บริษัท เห็นสมควร ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงการพัฒนา และแก้ไขเปลี่ยนแปลงให้ดีขึ้น โดยผู้ให้บริการจะบอกกล่าวล่วงหน้า หรือตกลงร่วมกันเป็นหนังสือระหว่างคู่สัญญาทั้งสองฝ่าย
- 1.4 ผู้ให้บริการให้คำรับรองต่อบริษัทเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการ ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงธรรมาภิบาลที่ดี (Good Corporate Governance) การประมวลผลข้อมูลส่วนบุคคล การรักษาความลับอย่างเคร่งครัด เมื่อสัญญาที่มีอยู่ใด ๆ สิ้นสุดลงหรือถูกบอกเลิกหรือเมื่อได้รับแจ้งจากบริษัท ผู้ให้บริการจะดำเนินการลบ และทำลายข้อมูลส่วนบุคคลทั้งหมด ด้วยวิธีการที่มีความมั่นคงปลอดภัยตามที่ตกลงกับบริษัท และตามกฎหมายที่เกี่ยวข้อง รวมถึง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด ทั้งนี้ ผู้ให้บริการจะคำนึงถึงความปลอดภัยของข้อมูลส่วนบุคคลอย่างถึงที่สุด
- 1.5 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า ข้อตกลงเพิ่มเติมฉบับนี้จะต้องอ่านร่วมกับสัญญาที่มีอยู่และประกอบเป็นส่วนหนึ่งของสัญญาที่มีอยู่ เว้นแต่จะกำหนดไว้เป็นอย่างอื่นในข้อตกลงเพิ่มเติมนี้ ทั้งนี้ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อกำหนดของสัญญาที่มีอยู่ ยังคงไม่เปลี่ยนแปลงและมีผลใช้บังคับอย่างสมบูรณ์

2. ข้อตกลงและเงื่อนไข

ในกรณีที่มีข้อขัดแย้งกันระหว่างข้อ 2 นี้กับข้อ 3 ของข้อตกลงเพิ่มเติมนี้เกี่ยวกับขอบเขตของหน้าที่ในการรักษาความลับของคู่สัญญาฝ่ายหนึ่งและ/หรือข้อยกเว้นการรักษาความลับที่ใช้บังคับใด ๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล ให้ข้อกำหนดและเงื่อนไขในข้อ 2 นี้ใช้บังคับ

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อกำหนดและเงื่อนไขต่อไปนี้จะบังคับเกี่ยวกับข้อมูลส่วนบุคคล

2.1 ข้อกำหนดทั่วไป

คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมให้ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้นผู้ให้บริการจึงตกลงที่จะปฏิบัติตามคำสั่งเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัทอย่างเคร่งครัด และจะไม่กระทำการใด ๆ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในนามของบริษัทโดยไม่ได้รับอนุญาตเป็นหนังสือล่วงหน้า และผู้ให้บริการจะปฏิบัติการอื่นใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

2.2 การประมวลผลข้อมูลส่วนบุคคล

ในการประมวลผลข้อมูลส่วนบุคคล ผู้ให้บริการในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ตกลงดังนี้

- (1) ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงแต่ไม่จำกัดเพียง นโยบายความเป็นส่วนตัว ข้อตกลงหรือแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล หรือการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในการให้บริการและการปฏิบัติตามหน้าที่อื่น ๆ ของตนภายใต้สัญญาที่มีอยู่ทั้งหมด
- (2) แจ้งให้พนักงาน ตัวแทน บุคลากรของตนทราบและดำเนินการให้แน่ใจว่าบุคคลเหล่านั้น ปฏิบัติตามคำสั่งของบริษัท และกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งหมดเท่านั้น
- (3) การประมวลผลข้อมูลส่วนบุคคลต้องทำภายใต้คำสั่งที่เป็นลายลักษณ์อักษรหรือมีบันทึกจากบริษัท เว้นแต่กรณีที่ผู้ให้บริการจะต้องปฏิบัติตามกฎหมาย
- (4) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทั้งปวงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามสมควร ตามรายละเอียดของเอกสารแนบท้าย 3 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

- (5) แจ้งให้บริษัททราบเป็นหนังสือทันทีโดยไม่ชักช้า เมื่อผู้ให้บริการทราบถึงกรณีดังต่อไปนี้
- การฝ่าฝืนอย่างร้ายแรงในการรักษาความปลอดภัยหรือมีเหตุที่น่าจะเชื่อว่าข้อมูลส่วนบุคคลอาจถูกเปิดเผย เข้าถึง หรือใช้โดยไม่ได้รับอนุญาต หรือมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
 - เมื่อมีคำร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
 - เมื่อมีหมายเรียก หรือคำสั่งจากศาล หรือเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐผู้มีอำนาจ หรือหน่วยงานกำกับดูแล เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- (6) ดำเนินการตามที่เหมาะสมและสมควร โดยค่าใช้จ่ายของผู้ให้บริการ รวมไปถึงแต่ไม่จำกัดเพียงการแจ้งบุคคลที่ได้รับผลกระทบ การเยียวยาผลกระทบ จากการที่ผู้ให้บริการไม่สามารถดำเนินการรักษาความปลอดภัยหรือป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตต่อข้อมูลส่วนบุคคลได้ และ
- (7) ไม่โอนข้อมูลส่วนบุคคลออกจาก หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากบุคคลอื่นที่อยู่นอกประเทศไทยโดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากบริษัทก่อน

2.3 การป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้ให้บริการรับรองและรับประกันว่า ณ วันที่ตกลงให้มีผลใช้บังคับและตลอดระยะเวลาของสัญญาที่มีอยู่ ผู้ให้บริการได้จัดให้มีและจะจัดให้มีการควบคุมเมื่อมีการลงข้อมูล การเข้าถึง การแทรกแซง การเปิดเผย การใส่รหัสและมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้มาตรฐานสากลและเพียงพอเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะปลอดภัยและคงไว้ซึ่งความลับ ซึ่งรวมถึง การได้รับการป้องกันจากการคุกคามหรือภัยอันตรายที่อาจมีขึ้นต่อความสมบูรณ์ของการเข้าถึงหรือใช้โดยไม่ได้รับอนุญาตซึ่งข้อมูลส่วนบุคคล

2.4 เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเกิดกับบริษัท และ/หรือผู้ให้บริการ และ/หรือผู้ให้บริการช่วง คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่าจะดำเนินการตามกฎหมาย

คุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด แจ้งให้คู่สัญญาอีกฝ่ายรับทราบในทันทีโดยไม่ชักช้า บรรเทาความเสียหาย รวมไปถึงแต่ไม่จำกัดเพียงให้ความช่วยเหลือ อำนาจความสะดวกซึ่งกันและกัน

3. การรักษาความลับ

3.1 ข้อจำกัดการใช้และการเปิดเผย

- (1) คู่สัญญาแต่ละฝ่ายตกลงจะรักษาข้อมูลที่เป็นความลับทั้งหมดของอีกฝ่ายหนึ่งไว้เป็นความลับอย่างเคร่งครัดและจะใช้มาตรการที่จำเป็นตามสมควรเพื่อรักษาข้อมูลที่เป็นความลับ รวมทั้ง
 - (1.1) ปฏิบัติตามมาตรการรักษาความปลอดภัยทั้งหมดที่กำหนดขึ้นเพื่อป้องกันข้อมูลที่เป็นความลับจากการเข้าถึงหรือการใช้โดยไม่ได้รับอนุญาต และ
 - (1.2) เก็บรักษาข้อมูลที่เป็นความลับทั้งหมดภายในการควบคุมของคู่สัญญาฝ่ายนั้น ทั้งนี้ ผู้รับข้อมูลจะต้องไม่ดำเนินการต่อไปนี้ โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้ข้อมูลก่อน
 - (ก) เปิดเผยข้อมูลที่เป็นความลับดังกล่าวแก่บุคคลภายนอก (ที่ไม่ใช่หน่วยงานกำกับดูแลที่มีอำนาจเหนือผู้รับข้อมูล) เว้นแต่จะได้รับอนุญาตโดยประการอื่นภายใต้สัญญาที่มีอยู่ หรือ
 - (ข) ใช้ข้อมูลความลับดังกล่าวเพื่อวัตถุประสงค์ใด ๆ ที่นอกเหนือไปจากการใช้สิทธิหรือการปฏิบัติตามหน้าที่ผูกพันของตนภายใต้สัญญาที่มีอยู่
- (2) คู่สัญญาแต่ละฝ่ายจะเปิดเผยข้อมูลที่เป็นความลับของอีกฝ่ายหนึ่งได้เฉพาะบุคคลหรือกรณีดังต่อไปนี้
 - (2.1) ให้แก่บุคลากรของตนที่เป็นพนักงาน ตัวแทน ที่จำเป็นต้องรู้ข้อมูลที่เป็นความลับดังกล่าวเพื่อใช้สิทธิของผู้รับข้อมูลดังกล่าวหรือเพื่อปฏิบัติตามหน้าที่ผูกพันของผู้รับข้อมูลดังกล่าวตามสัญญาที่มีอยู่
 - (2.2) ให้แก่หน่วยงานกำกับดูแลที่มีอำนาจเหนือผู้รับข้อมูล และ
 - (2.3) ตามที่ได้รับอนุญาตโดยประการอื่นภายใต้สัญญาที่มีอยู่

- (3) ในการใช้ข้อมูลที่เป็นความลับข้างต้น คู่สัญญาแต่ละฝ่ายจะต้องใช้ความพยายามตามสมควรที่จะช่วยเหลืออีกฝ่ายหนึ่งในการค้นหาหรือป้องกันการใช้หรือการเปิดเผยข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต
- (4) คู่สัญญาแต่ละฝ่ายจะต้องแจ้งให้อีกฝ่ายหนึ่งทราบทันทีโดยไม่ชักช้า และจะให้ความร่วมมือในการขอคำสั่งยับยั้งการกระทำที่ฝ่าฝืนความลับของข้อมูลความลับจากหน่วยงานที่มีอำนาจ ในกรณีที่ฝ่ายดังกล่าวทราบว่าหรือมีเหตุผลที่จะเชื่อได้ว่ามีบุคคลใด ๆ ที่ได้เข้าถึงข้อมูลที่เป็นความลับของฝ่ายดังกล่าว โดยฝ่าฝืนหรือมีเจตนาที่จะฝ่าฝืนข้อกำหนดของสัญญาที่มีอยู่
- (5) นอกจากนี้ ผู้รับข้อมูลอาจใช้หรือเปิดเผยข้อมูลที่เป็นความลับ (เว้นแต่ข้อมูลส่วนบุคคล) ตามขอบเขตที่ผู้รับข้อมูลดังกล่าวถูกบังคับตามกฎหมายให้เปิดเผยข้อมูลที่เป็นความลับดังกล่าวได้ โดยมีเงื่อนไขว่า ผู้รับข้อมูลจะต้องใช้ความพยายามตามสมควรที่จะบอกกล่าวล่วงหน้าเป็นหนังสือเกี่ยวกับการถูกบังคับให้เปิดเผยดังกล่าวแก่ผู้ให้ข้อมูล และจะต้องให้ความร่วมมือกับผู้ให้ข้อมูลในส่วนที่เกี่ยวข้องกับความพยายามใด ๆ ที่จะป้องกันหรือจำกัดขอบเขตของการเปิดเผยดังกล่าว

3.2 คู่สัญญาแต่ละฝ่ายจะต้องดำเนินการเพื่อให้แน่ใจว่า พนักงาน และตัวแทน ซึ่งรวมไปถึงผู้ให้บริการช่วงภายใต้สัญญาที่มีอยู่ของตน จะปฏิบัติตามข้อกำหนดในข้อตกลงเพิ่มเติมนี้ โดยเท่าที่บังคับใช้ได้ คู่สัญญาแต่ละฝ่ายจะต้องดำเนินการดังต่อไปนี้

- (1) ให้พนักงานหรือตัวแทนเข้าทำสัญญาหรือคำรับรองเป็นหนังสือกับตน โดยมีผลผูกพันพนักงาน หรือตัวแทน ซึ่งรวมไปถึงผู้ให้บริการช่วงภายใต้สัญญาที่มีอยู่ดังกล่าวตามข้อกำหนดในข้อตกลงเพิ่มเติมนี้ และ
- (2) จัดส่งสำเนาสัญญาหรือคำรับรอง ที่ได้ลงนามโดยพนักงาน หรือตัวแทน ซึ่งรวมไปถึงผู้ให้บริการช่วงภายใต้สัญญาที่มีอยู่ข้างต้นให้แก่บริษัท เมื่อบริษัทร้องขอ

4. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อผู้ให้บริการหรือผู้ให้บริการช่วง แล้วแต่กรณี เพื่อขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการตกลงที่จะแจ้งบริษัททันทีโดยไม่ชักช้า หรือผู้ให้บริการอาจดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ก็ต่อเมื่อผู้ให้บริการไม่สามารถติดต่อบริษัท และต้องดำเนินการข้างต้นโดยไม่อาจหลีกเลี่ยงได้ ทั้งนี้ ผู้ให้บริการต้องพิจารณาถึงปัจจัยต่าง ๆ ซึ่งรวมถึง กฎหมายคุ้มครองข้อมูลส่วนบุคคล โอกาสที่จะเกิดความเสียหายแก่บริษัท แนวทางปฏิบัติระหว่างคู่สัญญาทั้งสองฝ่าย โดยมีบันทึกการพิจารณาดังกล่าว

เป็นหลักฐานแล้ว ก่อนดำเนินการข้างต้น อนึ่ง บันทึกข้างต้นไม่ตัดสิทธิบริษัทที่จะเรียกร้องค่าเสียหายกับผู้ให้บริการ (ถ้ามี)

5. ภาษาและกฎหมายที่ใช้บังคับ

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ถือเอา [ภาษาไทย/ ภาษาอังกฤษ] เป็นภาษาหลักในการตีความและดำเนินการต่าง ๆ ซึ่งรวมไปถึงแต่ไม่จำกัดเพียง การส่งหนังสือบอกกล่าว การติดต่อสื่อสารระหว่างคู่สัญญาทั้งสองฝ่าย และการระงับข้อพิพาทโดยอนุญาโตตุลาการ โดยมี [กฎหมายไทย/ กฎหมายต่างประเทศ] เป็นกฎหมายที่ใช้บังคับแก่ข้อตกลงเพิ่มเติมฉบับนี้

6. ความสมบูรณ์ของข้อตกลงเพิ่มเติม

ในกรณีที่ข้อตกลงใด ข้อตกลงหนึ่ง ภายใต้ข้อตกลงเพิ่มเติมนี้ เป็นโมฆะ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่า ข้อตกลงอื่นภายใต้ข้อตกลงเพิ่มเติมนี้ที่ไม่เป็นโมฆะ มีผลบังคับใช้ระหว่างคู่สัญญาทั้งสองฝ่ายต่อไป และคู่สัญญาทั้งสองฝ่ายจะร่วมกันแก้ไขข้อตกลงที่มีผลเป็นโมฆะให้มีผลบังคับใช้ได้ตามกฎหมาย โดยให้มีผลในทางการค้าที่ใกล้เคียงกับข้อตกลงที่มีผลเป็นโมฆะนั้นมากที่สุดเท่าที่จะทำได้

7. การแก้ไขเปลี่ยนแปลง

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ การแก้ไขเปลี่ยนแปลงข้อตกลงเพิ่มเติมนี้ไม่สามารถกระทำได้ เว้นแต่จะทำขึ้นเป็นหนังสือและลงนามโดยคู่สัญญาทั้งสองฝ่าย หรือโดยการบอกกล่าวล่วงหน้าจากบริษัท โดยให้การเปลี่ยนแปลงดังกล่าวมีผลบังคับใช้ไม่เกิน [โปรดระบุระยะเวลา] นับแต่วันที่บริษัท ได้ส่งคำบอกกล่าวข้างต้น

8. ความรับผิดชอบสัญญา

คู่สัญญาแต่ละฝ่ายจะต้องรับผิดชอบค่าใช้จ่ายให้กับคู่สัญญาอีกฝ่ายหนึ่งสำหรับค่าปรับ ความสูญเสีย หรือความเสียหายทั้งหมดที่เกิดแก่คู่สัญญาฝ่ายที่ไม่ได้ทำผิดสัญญา อันเนื่องมาจากการที่คู่สัญญาอีกฝ่ายหนึ่งฝ่าฝืนหน้าที่ใด ๆ ภายใต้สัญญานี้

9. ความสิ้นสุดของข้อตกลงเพิ่มเติม

ข้อตกลงเพิ่มเติมนี้อาจสิ้นสุดได้โดยการตกลงร่วมกันระหว่างคู่สัญญาทั้งสองฝ่าย หรือการบอกกล่าวเป็นหนังสือล่วงหน้า ไม่เกิน [โปรดระบุระยะเวลา] นับแต่วันที่คู่สัญญาฝ่ายหนึ่งได้ส่งคำบอกกล่าวข้างต้น

เพื่อเป็นหลักฐานแห่งการนี้ คู่สัญญาทั้งสองฝ่ายภายใต้ข้อตกลงเพิ่มเติมนี้ ได้รับทราบและเข้าใจ คำรับรอง ข้อตกลงและเงื่อนไข ตลอดจนเอกสารแนบท้ายที่ได้ตกลงกันไว้ทั้งหมดแล้ว และได้ลงลายมือชื่อพร้อมประทับตราสำคัญ (หากมี) ด้านล่าง ในต้นฉบับข้อตกลงเพิ่มเติมนี้ จำนวนสองฉบับ โดยต่างฝ่ายต่างถือต้นฉบับไว้ฝ่ายละฉบับเพื่อเก็บไว้เป็นหลักฐาน

บริษัท: [ชื่อบริษัท]

ผู้ให้บริการ: [ระบุชื่อบริษัทผู้ให้บริการ] หรือ [ระบุชื่อผู้ให้บริการ]

ลงลายมือชื่อ:.....

ลงลายมือชื่อ:.....

ชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

ตำแหน่ง: _____

วันที่: _____

วันที่: _____

เอกสารแนบท้าย 1

สัญญาระหว่างคู่สัญญาทั้งสองฝ่ายที่มีอยู่ประกอบด้วยสัญญา/ เอกสารดังต่อไปนี้ (กรณารับ
รายละเอียดในตารางด้านล่าง – ไม่แนะนำให้ปล่อยว่างไว้)

ลำดับที่	ชื่อสัญญา/ เอกสาร	วันที่	หมายเหตุ

เอกสารแนบท้าย 2

รายละเอียดการประมวลผลข้อมูลส่วนบุคคล

ประเภทเจ้าของข้อมูลส่วนบุคคล

[ระบุ]

ประเภทข้อมูลส่วนบุคคลที่ประมวลผล

[ระบุ]

วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

[ระบุ]

ระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล

[ระบุ]

อื่น ๆ

[ระบุ]

เอกสารแนบท้าย 3

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้ให้บริการตกลงจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ดังนี้

[ขึ้นอยู่กับแต่ละบริษัท]

11.6 ตัวอย่างร่างคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

แบบคำร้องขอการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

[ระบุชื่อบริษัท]

เนื่องด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) ระบุให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิอันเกี่ยวข้องกับข้อมูลส่วนบุคคลของตนตามที่กำหนดไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อให้[ระบุชื่อบริษัท] (“บริษัท”) สามารถปฏิบัติหน้าที่ของตนในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลได้ บริษัทจึงได้จัดทำแบบคำร้องฉบับนี้ เพื่อจัดให้ท่านสามารถดำเนินการใช้สิทธิของท่าน โปรดระบุรายละเอียดดังต่อไปนี้

ส่วนที่ 1 ข้อมูลของผู้ยื่นคำร้องขอ

เพื่อยืนยันตัวตนของผู้ยื่นคำร้องขอ ขอให้ท่านโปรดใส่ข้อมูลของท่านตามที่ระบุไว้ดังต่อไปนี้

ชื่อนามสกุล	
ที่อยู่	
หมายเลขโทรศัพท์ที่ติดต่อได้	
อีเมล	

เพื่อประโยชน์ในการยืนยันตัวตนของผู้ยื่นคำร้องขอ บริษัทขอให้ท่านแสดงบัตรประชาชนตัวจริงของท่านในกรณีที่ท่านได้ยื่นคำร้องขอฉบับนี้ ทั้งนี้ หากเป็นการยื่นคำร้องขอโดยผ่านทางระบบอิเล็กทรอนิกส์หรือช่องทางอื่น ขอให้ท่านใส่เลขประจำตัวบัตรประชาชน 13 หลัก พร้อมวันที่ออกบัตรและวันที่บัตรหมดอายุ

เลขบัตรประชาชน	
วันที่ออกบัตร	

วันที่บัตรหมดอายุ	
-------------------	--

ส่วนที่ 2 สถานะของผู้ยื่นคำร้องขอ

ท่านเป็นเจ้าของข้อมูลส่วนบุคคลที่ต้องการใช้สิทธิตามคำร้องฉบับนี้

- [] ใช่ ข้าพเจ้าเป็นเจ้าของข้อมูลส่วนบุคคลและมีสิทธิตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ในการยื่นคำร้องขอฉบับนี้
- [] ไม่ใช่ ข้าพเจ้าดำเนินการในนามของผู้อื่น (ระบุชื่อ และเลขบัตรประจำตัวประชาชนหรือเลขหนังสือเดินทางของเจ้าของข้อมูลส่วนบุคคล พร้อมทั้งระบุเหตุผลในการดำเนินการแทน)

ชื่อ-สกุล	
เลข บั ต ร ป ระ จ ำ ต วั ประชาชน/เลขที่หนังสือ เดินทาง	
เหตุผลในการดำเนินการ แทน	

ในการยื่นคำร้องขอแทนหรือในนามเจ้าของข้อมูลส่วนบุคคลบริษัทสงวนสิทธิ์ในการพิจารณาคำร้องขอของท่านและอาจปฏิเสธคำร้องขอของท่าน เว้นแต่บริษัทมีหน้าที่ตามกฎหมายที่จะต้องพิจารณาและดำเนินการตามคำร้องขอของท่านที่จัดทำแทนหรือในนามเจ้าของข้อมูลส่วนบุคคลอื่น

ส่วนที่ 3 รายละเอียดของคำร้องขอ

ข้าพเจ้าต้องการยื่นคำร้องขอฉบับนี้ต่อบริษัท (ผู้ควบคุมข้อมูลส่วนบุคคล) ดังนี้

ตัวอย่าง

ข้าพเจ้าต้องการขอรับสำเนาข้อมูลเกี่ยวกับประวัติการเรียกร้องค่าสินไหมทดแทนของข้าพเจ้าทั้งหมด

เจ้าของข้อมูลส่วนบุคคลมีสถานะหรือความสัมพันธ์อย่างไรกับบริษัท

- | | | |
|--|---|--|
| ☐ ผู้สมัครงาน | ☐ พนักงาน | ☐ อดีตพนักงาน |
| ☐ ผู้เอาประกันภัย | ☐ ผู้รับประโยชน์ | ☐ ผู้ชำระเงินตามกรมธรรม์ประกันภัย |
| ☐ คู่ค้า | ☐ พนักงานของบริษัทคู่ค้า | |
| ☐ อื่น ๆ (โปรดระบุ) _____ | | |

ผู้ร้องขอต้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในเรื่องใด

- ☐ สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- ☐ สิทธิในการขอรับสำเนาข้อมูลส่วนบุคคล
- ☐ สิทธิขอให้เปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- ☐ สิทธิในการเพิกถอนความยินยอม (ใช้ได้เฉพาะเมื่อท่านได้ให้ความยินยอมไว้กับบริษัท)
- ☐ สิทธิในการแก้ไขหรือทำให้ข้อมูลเป็นปัจจุบัน
- ☐ สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล
- ☐ สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล
- ☐ สิทธิในการโอนย้ายข้อมูลส่วนบุคคล
- ☐ สิทธิในการคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล

[] สิทธิในการขอให้ดำเนินการให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

[] กรณีข้อร้องเรียนอื่นที่เกี่ยวข้อง

หมายเหตุ ขอให้ท่านโปรดระวังว่าการเลือกใช้สิทธิของท่านมากกว่า 1 สิทธิซึ่งอาจทำให้เกิดความสับสนของบริษัทในการปฏิบัติตามคำขอของท่าน หากท่านเลือกใช้สิทธิมากกว่า 1 สิทธิท่านสามารถเขียนระบุเพิ่มเติมอธิบายถึงการเลือกใช้สิทธิของท่าน

ขอให้ท่านโปรด อธิบายรายละเอียดที่เกี่ยวข้องกับคำร้องขอนั้น

ตัวอย่าง

ข้าพเจ้าขอให้บริษัทส่งสำเนารายละเอียดเกี่ยวกับการเรียกร้องค่าสินไหมทดแทนของข้าพเจ้าไปให้บริษัทประกันภัยเอ ด้วย

ส่วนที่ 4 การดำเนินงานของบริษัทภายหลังจากที่ได้รับคำร้องขอ

บริษัทขอขอบคุณที่ท่านกรุณาส่งคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลพร้อมทั้งเอกสารและรายละเอียดที่เกี่ยวข้อง ทั้งนี้ บริษัทจะพิจารณาเรื่องดังกล่าวและดำเนินการติดต่อกลับไปภายในระยะเวลาที่กฎหมายกำหนด หากมีกรณีที่บริษัทอาจต้องการคำอธิบายเพิ่มเติมหรือต้องโต้แย้งการใช้สิทธิของท่าน บริษัทจะดำเนินการติดต่อท่านกลับไปตามรายละเอียดที่ท่านได้ให้ไว้ในส่วนที่ 1 ภายในระยะเวลาที่กฎหมายกำหนด

ทั้งนี้ บริษัทขอสงวนสิทธิในการปฏิเสธหรือระงับการปฏิบัติตามคำขอของท่านเฉพาะในกรณีดังต่อไปนี้

- 1) บริษัทไม่มีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับท่าน
- 2) คำร้องขอของท่านไม่อาจแสดงได้ว่าท่านต้องการใช้สิทธิอะไร หรือท่านมีสิทธิตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลอย่างไร
- 3) ท่านไม่สามารถแสดงให้เห็นอย่างชัดเจนได้ว่าผู้ยื่นคำร้องเป็นเจ้าของข้อมูล หรือมีอำนาจในการยื่นคำร้องดังกล่าว

- 4) ด้วยหน้าที่หรือข้อกำหนดตามกฎหมายบริษัทไม่สามารถให้ข้อมูลหรือดำเนินการตามคำร้องขอของท่าน
- 5) คำร้องขอของท่านไม่เป็นไปตามเงื่อนไขที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด หรือบริษัทมีเหตุในการปฏิเสธการดำเนินการตามสิทธิของท่านตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดไว้ และบริษัทสามารถใช้เหตุดังกล่าวได้โดยชอบด้วยกฎหมาย

ส่วนที่ 5 คำรับรอง

ข้าพเจ้าขอยืนยันว่าข้าพเจ้าได้อ่านและเข้าใจเนื้อหาและข้อกำหนดตามที่ระบุไว้ในคำร้องขอฉบับนี้ พร้อมทั้งรับรองว่าข้อมูลดังกล่าวที่ข้าพเจ้าให้ไว้ตามเอกสารฉบับนี้ถูกต้อง ครบถ้วนและสมบูรณ์ ข้าพเจ้าขอยืนยันและรับประกันว่าในการใช้สิทธิตามเอกสารฉบับนี้ ข้าพเจ้ามีสิทธิอย่างถูกต้องตามกฎหมาย ข้าพเจ้าไม่มีเจตนาดำเนินการเพื่อก่อให้เกิดความเสียหายกับบุคคลใดหรือกับบริษัท ข้าพเจ้าจึงได้ลงลายมือชื่อตามที่ระบุด้านล่างนี้

ลายมือชื่อ _____

ชื่อ _____

วันที่ _____

ท่านสามารถติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่ [ระบุช่องทางการติดต่อ]

11.7 ตัวอย่างร่างการแจ้งเหตุละเมิดต่อเจ้าของข้อมูลส่วนบุคคล

****รายละเอียดร่างการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคลต่อไปนี้ เป็นเพียงตัวอย่างร่างข้อความเท่านั้น สำหรับรายละเอียดการแจ้งดังกล่าวและชื่อยกเว้นนั้น จะต้องมีการปรับแก้ให้เป็นไปตามประกาศของคณะกรรมการ¹⁰⁹ ต่อไป****

[หัวกระดาษบริษัท]

[วัน/เดือน/ปี]¹¹⁰

เรื่อง การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เรียน [ลูกค้าคนสำคัญของเรา]

[ชื่อบริษัท] ขอแจ้งให้ท่านทราบว่า ความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลของท่านเป็นเรื่องที่บริษัทให้ความสำคัญเป็นอันดับแรก โดยไม่มีชื่อยกเว้นใด ๆ ทั้งนี้ ทางเราจึงได้จัดให้มีและพัฒนามาตรการคุ้มครองความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลของท่านอย่างสม่ำเสมอ เพื่อให้เราสามารถปกป้องและคุ้มครองความไว้วางใจของท่านที่ได้ให้ไว้กับเรา

อย่างไรก็ตาม แม้ว่าเราจะได้พยายามคุ้มครองและป้องกันข้อมูลส่วนบุคคลของท่านอย่างสุดความสามารถของเราแล้วก็ตาม เรามีความเสียใจที่จะต้องแจ้งให้ท่านทราบว่า รายละเอียดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลเท่าที่ทราบ เช่น

- รายละเอียดประเภทข้อมูลส่วนบุคคลที่อาจได้รับผลกระทบ
- ลักษณะของการละเมิดข้อมูลส่วนบุคคล

ตัวอย่าง “ได้มีการเข้าถึงข้อมูลบัตรเครดิตของท่านโดยบุคคลภายนอกที่ไม่ได้รับอนุญาต”¹¹¹ ซึ่งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้อาจส่งผลกระทบในทางใด ๆ ต่อท่านได้ ในฐานะที่ท่านเป็นลูกค้าคนสำคัญของเรา เราจึงรีบดำเนินการแจ้งให้ท่านอย่างเร็วที่สุดเท่าที่เราจะทำได้ โดยในขณะนี้ ทางเราและผู้เชี่ยวชาญกำลังดำเนินการตรวจสอบและแก้ไขสถานการณ์ดังกล่าวอย่างเต็มความสามารถ ภายใต้ความดูแลของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

¹⁰⁹ มาตรา 37 (4) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹¹⁰ ข้อสังเกต: ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องแจ้งโดยไม่ชักช้า

¹¹¹ ข้อสังเกต: บริษัท จะต้องระมัดระวังในการให้ข้อเท็จจริงในกรณีนี้ เช่น เวลาเกิดเหตุ เพราะข้อเท็จจริงเหล่านี้อาจถูกใช้เป็นหลักฐานในการกล่าวหาบริษัทได้ในอนาคต

นอกจากนี้ เราได้ระบุนายละเอียดที่เกี่ยวข้องพร้อมแนวทางในการเยียวยาเหตุการณ์ละเมิดข้อมูลส่วนบุคคลข้างต้น เพื่อแก้ไขและบรรเทาผลกระทบที่อาจเกิดขึ้นกับท่านและข้อมูลส่วนบุคคลของท่านไว้แล้ว ในเว็บไซต์ของเรา: [แทรกลิงก์ ไปยังรายละเอียดแนวทางการเยียวยาเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในเว็บไซต์ของบริษัท]¹¹²

ในกรณีที่ท่านมีข้อสงสัยเพิ่มเติม โปรดติดต่อบริษัท [ระบุชื่อบริษัท] ได้ที่:

อีเมล: [แทรก Email Address]

หมายเลขโทรศัพท์: [หมายเลขโทรศัพท์ Call Center] ซึ่งสามารถติดต่อได้ในเวลาทำการระหว่างเวลา [ระบุช่วงเวลา]

เราเข้าใจดีว่า ท่านอาจมีความกังวลใจเกี่ยวกับความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลของท่าน ดังนั้น เราจะเร่งแก้ไขสถานการณ์ดังกล่าวให้เร็วที่สุดเท่าที่จะทำได้ โดยที่เราหวังเป็นอย่างยิ่งว่า ท่านจะยังคงให้ความไว้วางใจกับเราต่อไปในอนาคต

ขอแสดงความนับถือ

[ในนามของบริษัท]

¹¹² ข้อสังเกต: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งแนวทางการเยียวยาพร้อมกับรายละเอียดของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลด้วย

11.8 ตัวอย่างการแจ้งช่องทางการถอนความยินยอมตามมาตรา 95

การแจ้งรายละเอียดอันเกี่ยวข้องกับข้อมูลส่วนบุคคลของท่าน

[ระบุชื่อบริษัท]

[*วันที่ก่อนวันที่ 1 มิถุนายน 2565]

เรียน [ลูกค้าคนสำคัญของเรา]

[บทนำ – ซึ่งพูดถึงชื่อบริษัท ข้อมูลการประกอบธุรกิจ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง]

[บริษัท] ขอแจ้งให้ท่านทราบว่าบริษัทได้มีเก็บรวบรวม ใช้ หรือเปิดเผย (รวมเรียกว่า “**ประมวลผล**”) ข้อมูลส่วนบุคคลของท่าน เช่น [ชื่อ นามสกุล ที่อยู่ และหมายเลขโทรศัพท์] ไว้ในความครอบครองของบริษัท ก่อนหน้าวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ทั้งฉบับ (“**พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**”)

ดังนั้น เพื่อแจ้งและสร้างความเข้าใจถึงวัตถุประสงค์พร้อมทั้งข้อมูลอื่นที่เกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคลของท่าน และสิทธิของท่านตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทได้จัดทำนโยบายความเป็นส่วนตัว [แทรกลิงก์ สำหรับ Privacy Policy/หรือแนบ] ซึ่งบริษัทขอให้ท่านโปรดใช้เวลาในการอ่าน และทำความเข้าใจข้อมูลดังกล่าวเพื่อประโยชน์ของท่านเอง

นอกจากนี้ เพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ดังกล่าว ท่านสามารถขอถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของท่านได้ โดยคลิก [แทรก Opt-Out Link] หรือติดต่อบริษัท ที่ [แทรก Email Address] อย่างไรก็ดี การที่ท่านเลือกที่จะถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของท่าน ในบางกรณีอาจเป็นอุปสรรคต่อความสามารถในการทำธุรกรรมระหว่างบริษัทกับท่าน หรือต่อการให้บริการของเราต่อท่าน หรือต่อการตอบสนองต่อข้อร้องขออื่น ๆ ของท่านได้ เช่น บริษัทอาจไม่สามารถให้บริการต่าง ๆ เกี่ยวกับผลิตภัณฑ์ หรือบริการของบริษัท รวมถึงการให้บริการเกี่ยวกับการเรียกร้องค่าสินไหมทดแทนให้แก่ท่านได้

ทั้งนี้ เมื่อบริษัทได้รับคำขอจากท่าน บริษัทจะพิจารณาและดำเนินการตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด และหากบริษัทไม่ได้รับการติดต่อจากท่านก่อนวันที่ 31 พฤษภาคม 2565 บริษัทขอเรียนใช้โอกาสนี้แจ้งให้ท่านทราบว่าบริษัทจะดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านต่อไป ซึ่งรวมไปถึงการเก็บรวบรวม ใช้ และการเปิดเผยต่อบุคคลภายนอก ทั้งนี้ ตามที่กำหนดไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และนโยบายความเป็นส่วนตัวของบริษัท

ขอแสดงความนับถือ

[ในนามของบริษัท]

11.9 ตัวอย่างแบบการบันทึกการประมวลผลข้อมูลส่วนบุคคล

	รายละเอียดกิจกรรมการประมวลผลข้อมูล			Who ใคร
	ลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	ฝ่ายงานที่เกี่ยวข้อง	ชื่อเอกสารที่เกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคล	เจ้าของข้อมูลส่วนบุคคล
	ระบุกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	ระบุฝ่ายงาน หรือส่วนงานที่เกี่ยวข้องกับกิจกรรมการประมวลผลนี้		เช่น พนักงาน บุคคลภายนอก (ผู้สมัครงาน ผู้ขายสินค้า ผู้ให้บริการ ตัวแทนจำหน่าย ลูกค้า)
ตัวอย่าง	การเก็บ Leads เพื่อเสนอขายทางโทรศัพท์	ฝ่าย Telemarketing	ไม่มี	ผู้มุ่งหวัง

What อะไร				
แหล่งที่มาของข้อมูลส่วนบุคคล	ประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	ประเภทของข้อมูลส่วนบุคคลที่มีความอ่อนไหวการ เก็บรวบรวม	วัตถุประสงค์ของการเก็บรวบรวม ใช้ เปิดเผย ข้อมูล ส่วนบุคคล	วัตถุประสงค์ของการเก็บรวบรวม ใช้ เปิดเผย ข้อมูล ส่วนบุคคลที่มีความอ่อนไหว
เช่น 1. เก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล 2. เก็บรวบรวมจากแผนกหรือส่วนงานอื่นในองค์กร เดียวกัน (โปรตระกูลซื้อแผนก) 3. เก็บรวบรวมจากบริษัทในเครือ (โปรตระกูลซื้อบริษัท) 4. เก็บรวบรวมจากแหล่งอื่น (โปรตระกูลซื้อบริษัทหรือ ประเภทของบุคคลที่รับข้อมูลส่วนบุคคลมา)		ข้อมูลส่วนบุคคลที่มีความอ่อนไหว หมายความว่ารวมถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความ คิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือ ปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูล สุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูล พันธุกรรม ข้อมูลชีวภาพ	เช่น 1. เพื่อการตลาด เช่นเพื่อการส่งเสริมสินค้า การโฆษณาเพื่อการขาย การสมัครสมาชิก การสมัครเพื่อรับข่าวสาร และอื่นๆ 2. เพื่อการปฏิบัติตามที่กฎหมายกำหนด เช่น พ.ร.บ. คุ้มครองแรงงาน 3. เพื่อการปฏิบัติตามสิทธิและหน้าที่ในสัญญา เช่น สัญญากับผู้รับจ้าง สัญญาให้บริการ สัญญาจ้างแรงงาน สัญญาซื้อขาย และอื่นๆ 4. เพื่อการให้บริการแก่ลูกค้า 5. เพื่อวัตถุประสงค์อื่น (ถ้ามี โปรดระบุ) (ถ้าข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมมา ถูกโอนหรือส่งต่อ กรุณาระบุวัตถุประสงค์เพื่อการโอนหรือส่งต่อด้วย)	
1. เก็บจากแหล่งอื่น - เก็บ Leads จากบริษัทคู่ค้า	1. ชื่อและนามสกุล 2. เลขบัตรประจำตัวประชาชน หรือข้อมูลใน	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว	1. เพื่อเสนอขายผลิตภัณฑ์ประกันภัย	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ฐานของกฎหมายเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	ฐานของกฎหมายเพื่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว	การแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล	การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
1. ความยินยอม 2. เป็นความจำเป็นเพื่อการปฏิบัติตามสัญญา (มีสัญญาเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล) 3. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ 4. เป็นการปฏิบัติตามกฎหมาย 5. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล 6. เป็นการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมาย (เช่น การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลเพื่อป้องกันการทุจริต ฉ้อโกง)	1. ความยินยอมอย่างชัดแจ้ง 2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ 3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล 4. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย 5. เป็นการปฏิบัติตามกฎหมาย เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกัน การประเมินความสามารถในการทำงานของลูกจ้าง ประโยชน์สาธารณะด้านการสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัยสถิติ ประโยชน์สาธารณะที่สำคัญ		1. แบบความยินยอม (แบบกระดาษ) 2. แบบความยินยอม (แบบอิเล็กทรอนิกส์) 3. แบบความยินยอม (ทั้งแบบกระดาษและแบบอิเล็กทรอนิกส์) 4. อื่น ๆ โปรดระบุ
1. เพื่อเสนอขายผลิตภัณฑ์ประกันภัย - ความยินยอม	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว	บริษัทได้แจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ	มีการขอความยินยอมผ่านทางแอปพลิเคชัน

ระบบ และสถานที่เก็บรักษาข้อมูลส่วนบุคคลที่เกี่ยวข้อง		
	หน่วยงานภายใน	
	ข้อมูลส่วนบุคคล ถ้าข้อมูลส่วนบุคคลถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายใน ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ไปยังแผนกการเงินและบัญชี (ส่งต่อในรูปแบบกระดาษ) หรือ ไปยังฝ่ายการตลาด (ส่งต่อในรูปแบบกระดาษ/รูปแบบอิเล็กทรอนิกส์)) กรุณาระบุชื่อแผนก หรือหน่วยงานภายในนั้นด้วย (ถ้ามี)	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถ้าข้อมูลส่วนบุคคลที่มีความอ่อนไหวถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายใน ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ไปยังแผนกการเงินและบัญชี (ส่งต่อในรูปแบบกระดาษ) หรือ ไปยังฝ่ายการตลาด (ส่งต่อในรูปแบบกระดาษ/รูปแบบอิเล็กทรอนิกส์)) กรุณาระบุชื่อแผนก หรือหน่วยงานภายในนั้นด้วย (ถ้ามี)
ระบบ A	ไม่มีการเปิดเผยข้อมูลส่วนบุคคลไปยังฝ่ายอื่น	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว

Where ที่ไหน			
การเปิดเผย หรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอก			
องค์กรภายนอก (ภายในประเทศไทย)		องค์กรภายนอก (ภายนอกประเทศไทย)	
ข้อมูลส่วนบุคคล ถ้าข้อมูลส่วนบุคคลถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายนอก ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ฝ่ายขาย ส่งข้อมูลส่วนบุคคลในรูปแบบ กระดาษไปยังบริษัทรับจัดทำบัญชี หรือ ไปยังบริษัทรับจัดเก็บเอกสาร (ส่งต่อในรูปแบบกระดาษ) กรุณาระบุชื่อหน่วยงานภายนอก หรือบริษัทนั้นด้วย (ถ้ามี)	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถ้าข้อมูลส่วนบุคคลถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายนอก ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ฝ่ายขาย ส่งข้อมูลส่วนบุคคลในรูปแบบ กระดาษไปยังบริษัทรับจัดทำบัญชี หรือ ไปยังบริษัทรับจัดเก็บเอกสาร (ส่งต่อในรูปแบบกระดาษ) กรุณาระบุชื่อหน่วยงานภายนอก หรือบริษัทนั้นด้วย (ถ้ามี)	ข้อมูลส่วนบุคคล ถ้าข้อมูลส่วนบุคคลถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายนอก ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ฝ่ายขาย ส่งข้อมูลส่วนบุคคลในรูปแบบ กระดาษไปยังบริษัทรับจัดทำบัญชี หรือ ไปยังบริษัทรับจัดเก็บเอกสาร (ส่งต่อในรูปแบบกระดาษ) กรุณาระบุชื่อหน่วยงานภายนอก หรือบริษัทนั้นด้วย (ถ้ามี)	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ถ้าข้อมูลส่วนบุคคลถูกเก็บไว้หลายรูปแบบ กรุณาระบุบุคคล/หน่วยงานภายนอก ที่ได้รับหรือเข้าถึงข้อมูลส่วนบุคคล ในรูปแบบใด (เช่น ฝ่ายขาย ส่งข้อมูลส่วนบุคคลในรูปแบบ กระดาษไปยังบริษัทรับจัดทำบัญชี หรือ ไปยังบริษัทรับจัดเก็บเอกสาร (ส่งต่อในรูปแบบกระดาษ) กรุณาระบุชื่อหน่วยงานภายนอก หรือบริษัทนั้นด้วย (ถ้ามี)
ไม่มีการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว	ไม่มีการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก	ไม่มีการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว

When เมื่อใด		
ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล	การอัปเดต หรือแก้ไขข้อมูลส่วนบุคคล	วัน และเวลาที่มีการลบ หรือทำลายข้อมูลส่วนบุคคล
กรณีระบุระยะเวลาที่ข้อมูลส่วนบุคคลจะถูกเก็บไว้ ถ้าไม่สามารถระบุระยะเวลาได้ กรณีระบุระยะเวลาที่พึงคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม ถ้าแต่ละแผนกมีระยะเวลาการเก็บเอกสาร (กระดาษ/อิเล็กทรอนิกส์) ที่แตกต่างกัน กรุณาชี้แจงรายละเอียดและแจ้งระยะเวลาการเก็บข้อมูลส่วนบุคคลตาม format นั้น ๆ	ถ้ามีกระบวนการหรือช่องทางสำหรับการทำให้ข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่ถูกเก็บรวบรวมมาให้เป็นปัจจุบัน กรุณาอธิบาย ถ้าไม่มีกระบวนการดังกล่าว กรุณาระบุ "ไม่มี" เช่น ข้อมูลส่วนบุคคลจะถูกทำให้เป็นปัจจุบันเมื่อได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคล หรือ ข้อมูลส่วนบุคคลจะถูกทำให้เป็นปัจจุบันทุกปี	
	มีการอัปเดตข้อมูลส่วนบุคคลปีละ 1 ครั้ง	

How อย่างไร	
การจัดช่องทางให้เจ้าของข้อมูลส่วนบุคคลดำเนินการตามสิทธิ	การร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
คำขอของเจ้าของข้อมูลส่วนบุคคล	
1. สิทธิขอให้ดำเนินการให้ข้อมูลส่วนบุคคลถูกต้องและเป็นปัจจุบัน 2. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 3. สิทธิขอให้ลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ 4. สิทธิการระงับการใช้ข้อมูลส่วนบุคคล 5. สิทธิการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุม หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคล 6. สิทธิขอให้โอนข้อมูลส่วนบุคคล	

11.10 ตัวอย่างคำรับรองสำหรับผู้ถือกรรมธรรม์ประกันภัยกลุ่ม หนังสือรับรองการได้รับความยินยอมจากสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ

คำรับรองสำหรับผู้ถือกรรมธรรม์ประกันภัยกลุ่ม

หนังสือรับรองการได้รับความยินยอมจากสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ

ทำที่ _____

วันที่ _____

บริษัท _____ (“บริษัท”)

สำนักงานเลขที่ _____

ขอรับรองว่า บริษัทได้แจ้ง นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้รับประกันภัยให้กับสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ รวมถึงบริษัทในเครือ (ถ้ามี) รับทราบแล้ว และข้อมูลของสมาชิกผู้เอาประกันภัยที่ส่งให้ผู้รับประกันภัย และ/หรือ นายหน้าประกันวินาศภัย และ/หรือ ตัวแทนประกันวินาศภัย เป็นข้อมูลที่ต้องและได้รับความยินยอมจากสมาชิกผู้เอาประกันภัย/สมาชิกสมทบก่อนการนำส่งข้อมูลให้กับผู้รับประกันภัยและ/หรือ นายหน้าประกันวินาศภัย และ/หรือ ตัวแทนประกันวินาศภัยเป็นที่เรียบร้อยแล้ว สำหรับกรรมธรรม์ประกันภัยกลุ่ม _____ ซึ่งเริ่มมีความคุ้มครองตั้งแต่วันที่ _____

ดังมีรายละเอียดต่อไปนี้

1. สมาชิกผู้เอาประกันภัย/สมาชิกสมทบ ยินยอมให้บริษัท และ/หรือ นายหน้าประกันวินาศภัย เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวของสมาชิกผู้เอาประกันภัย เพื่อวัตถุประสงค์ในการทำประกันภัย การตรวจสอบสุขภาพ การเรียกร้องหรือพิจารณาค่าสินไหมทดแทน และการปฏิบัติตามเงื่อนไขในกรรมธรรม์ รวมถึงการใด ๆ อันเกี่ยวกับธุรกิจประกันภัย โดยการเปิดเผยข้อมูลดังกล่าว ให้รวมถึงแต่ไม่จำกัดเพียง สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) บริษัทประกันภัย ตัวแทนประกันวินาศภัย หรือนายหน้าประกันวินาศภัย บริษัทรับประกันภัยต่อ คู่ค้าหรือผู้ให้บริการของบุคคลดังกล่าว

2. สมาชิกผู้เอาประกันภัย/สมาชิกสมทบ ยินยอมให้ผู้รับประกันภัย และ/หรือนายหน้าประกันวินาศภัย และ/หรือตัวแทนประกันวินาศภัย เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวของสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ เพื่อวัตถุประสงค์ในการทำประกันภัย การตรวจสอบสุขภาพ การเรียกร้องค่า

สินไหมทดแทน การปฏิบัติตามเงื่อนไขในกรรมธรรม์ รวมถึงการใด ๆ อันเกี่ยวกับธุรกิจประกันภัย โดยการเปิดเผยข้อมูลดังกล่าว ให้รวมถึงแต่ไม่จำกัดเพียง สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ตัวแทนประกันวินาศภัย นายหน้าประกันวินาศภัย บริษัทรับประกันภัยต่อ ผู้ถือกรรมธรรม์ และคู่ค้าหรือผู้ให้บริการของบุคคลดังกล่าว

3. สมาชิกผู้เอาประกันภัย/สมาชิกสมทบ ยินยอมให้แพทย์ หรือบุคลากรทางการแพทย์ หรือสถานพยาบาล หรือผู้รับประกันภัยอื่น หรือบุคคลอื่นใด ซึ่งมีประวัติและ/หรือข้อมูลสุขภาพของสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ เปิดเผยข้อมูลอ่อนไหวให้แก่ผู้รับประกันภัยหรือผู้แทนของผู้รับประกันภัย และ/หรือนายหน้าประกันวินาศภัย และ/หรือตัวแทนประกันวินาศภัยเพื่อการทำประกันภัย หรือการพิจารณาสินไหมตามกรรมธรรม์ประกันภัยได้

บริษัทตกลงที่จะจัดการให้สมาชิกผู้เอาประกันภัย/สมาชิกสมทบ ให้ความยินยอมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวเพื่อการทำประกันภัยกลุ่ม ซึ่งบริษัทจะจัดเก็บหลักฐานความยินยอมของสมาชิกผู้เอาประกันภัยไว้ตลอดเวลา และสามารถให้สำเนาแก่ผู้รับประกันภัย และ/หรือนายหน้าประกันวินาศภัย และ/หรือตัวแทนประกันวินาศภัยได้เมื่อร้องขอ

ในกรณีที่สมาชิกถอนความยินยอม บริษัทมีหน้าที่ต้องแจ้งให้ ผู้รับประกันภัยและ/หรือนายหน้าประกันวินาศภัยและ/หรือตัวแทนประกันวินาศทราบโดยไม่ชักช้า และบริษัทต้องช่วยอำนวยความสะดวกแก่ผู้รับประกันภัยและ/หรือนายหน้าประกันวินาศภัยและ/หรือตัวแทนประกันวินาศภัยในการติดต่อสมาชิกผู้เอาประกันภัย/สมาชิกสมทบ และแจ้งให้สมาชิกผู้เอาประกันภัยทราบว่า การเพิกถอนความยินยอมนี้อาจส่งผลให้ผู้รับประกันภัยไม่สามารถปฏิบัติหน้าที่หรือภาระผูกพันที่มีต่อสมาชิกผู้เอาประกันภัย/สมาชิกสมทบตามกรรมธรรม์ทั้งหมดหรือบางส่วนได้

บริษัทจะรับผิดชอบตามกฎหมายต่อนายหน้าประกันวินาศภัย และ/หรือผู้รับประกันภัย ผู้รับประกันภัย และ/หรือ นายหน้าประกันวินาศภัย และ/หรือ ตัวแทนประกันวินาศภัย หากบริษัทดำเนินการใดที่เป็นการขัดหรือแย้งกับคำรับรอง และ/หรือกฎหมาย ดังกล่าว ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล



ลงชื่อ _____ กรรมการผู้มีอำนาจ / ผู้รับมอบอำนาจ
()

บริษัท.....

บทที่ 12 เอกสารแนบ

12.1 แนวทางการปฏิบัติด้านทรัพยากรบุคคล

สำหรับการคุ้มครองข้อมูลส่วนบุคคลในการจ้างงานและปฏิบัติตามสัญญาจ้างแรงงานระหว่างพนักงานกับบริษัท ซึ่งส่วนหนึ่งในการปฏิบัติงานสำหรับฝ่ายทรัพยากรบุคคลของบริษัท สามารถแบ่งตามขั้นตอนได้ดังต่อไปนี้

12.1.1 การรับสมัครงาน (Recruitment)

ในขั้นตอนนี้ ผู้สมัครแต่ละรายที่ให้ข้อมูลของตนเองก็มีฐานะเป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งบริษัทที่ทำการประมวลผลข้อมูลส่วนบุคคลดังกล่าวเพื่อรับสมัครพนักงานนั้น มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ กระบวนการนี้ บริษัทควรจะต้องพิจารณาประเด็นดังต่อไปนี้

ตัวอย่างประเภทข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลทั่วไป	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว
➤ ชื่อ-นามสกุล ➤ อายุ ➤ เลขบัตรประจำตัวประชาชน ➤ เลขบัตรประจำตัวผู้ประกันตน/ สมาชิกประกันสังคม ➤ ที่อยู่ตามทะเบียนบ้าน/ ปัจจุบัน ➤ หมายเลขโทรศัพท์บ้าน/ มือถือ ➤ อีเมล ➤ ชื่อและนามสกุลบิดา/ มารดา ➤ เลขทะเบียนรถ ➤ เลขบัตรใบอนุญาตนุรักษ์รถยนต์/ จักรยานยนต์ ➤ อาชีพ ➤ สถานที่ทำงานปัจจุบัน ➤ ลายมือชื่อผู้สมัคร ➤ เลขบัญชีธนาคารที่ใช้รับเงินเดือน	➤ เชื้อชาติ ➤ ศาสนา ➤ ข้อมูลเกี่ยวกับความพิการ ➤ ข้อมูลเกี่ยวกับการกระทำความผิดอาญา/ ประวัติอาชญากรรม

➤ ประวัติการรับราชการทหาร (สำหรับผู้ชาย)	
--	--

ข้อสังเกต

กรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นที่ไม่ใช่ผู้สมัคร เช่น บิดา มารดา ภรรยา หรือบุตร ในใบสมัครงาน เป็นกรณีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวนี้สามารถอ้างฐานประโยชน์อันชอบธรรม (Legitimate Interest) ได้ โดยที่บริษัทจะต้องสามารถอธิบายได้ว่า บริษัทมีความจำเป็นอย่างไรที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นที่ไม่ใช่ผู้สมัคร เช่น จำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของภรรยาเพื่อใช้ติดต่อในเวลาฉุกเฉิน หรือจำเป็นจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบิดาหรือมารดาเพื่อใช้ประกอบการลดหย่อนภาษีให้พนักงาน

ทั้งนี้ หากข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นสำหรับการรับสมัครงาน บริษัท ไม่ควรเก็บรวบรวมข้อมูลส่วนบุคคลเหล่านั้น บ่อยครั้งที่บริษัท มักจะมีแบบฟอร์มรับสมัครงานที่กำหนดให้ผู้สมัครงานระบุข้อมูลส่วนบุคคลจนมากเกินไปเกินความจำเป็นในการพิจารณาการรับเข้าทำงาน เช่น หมู่เลือด ประวัติการศึกษาชั้นอนุบาล เป็นต้น ซึ่งขัดต่อหลักการประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อวัตถุประสงค์เท่านั้น ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ดังนั้น บริษัท ควรจะต้องพิจารณาปรับปรุงแบบฟอร์มรับสมัครงาน ให้เก็บรวบรวมเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต่อการพิจารณาการรับเข้าทำงานเท่านั้น เพื่อลดปริมาณและประเภทข้อมูลส่วนบุคคลที่ไม่จำเป็น

ฐานในการประมวลผลข้อมูลส่วนบุคคลของผู้สมัครงาน

ข้อมูลส่วนบุคคลทั่วไป	ข้อมูลส่วนบุคคลที่มีความอ่อนไหว
➤ ฐานประโยชน์โดยชอบด้วยกฎหมาย เช่น การประมวลผลข้อมูลส่วนบุคคลของผู้ติดต่อฉุกเฉิน การยื่นข้อเสนองาน (บริษัท เสนองานให้ก่อนที่เจ้าของข้อมูลส่วนบุคคลจะสมัครงาน) ➤ ฐานสัญญา (ความจำเป็นเพื่อดำเนินการตามคำขอในการเข้าทำสัญญาของเจ้าของข้อมูลส่วนบุคคล) เช่น การดำเนินการต่าง ๆ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้สมัครงานก่อน	➤ ฐานความยินยอมโดยชัดแจ้ง

12.1.2 การสัมภาษณ์ (Interview)

ในขั้นตอนการสัมภาษณ์ จะต้องมีการประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งโดยส่วนใหญ่แล้วข้อมูลส่วนบุคคลที่บริษัทประมวลผลในขั้นตอนนี้ ก็จะเป็นข้อมูลส่วนบุคคลชุดเดียวกับในขั้นตอนการสมัครงาน ทั้งนี้ บริษัทอาจอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลฐานเดียวกับฐานในการประมวลผลสำหรับขั้นตอนการสมัครงานได้

12.1.3 การเข้าทำสัญญาจ้างงาน

บริษัทอาจมีประเด็นที่ต้องพิจารณาดังนี้

- ในช่วงก่อนจ้างงานตามสัญญา บริษัทอาจกำหนดให้ผู้ที่จะผ่านการคัดเลือกเข้าตรวจสอบสุขภาพกับโรงพยาบาลที่บริษัททำสัญญาไว้ โดยกำหนดให้โรงพยาบาลส่งผลการตรวจสอบสุขภาพมายังบริษัท โดยตรงไม่ผ่านเจ้าของข้อมูลส่วนบุคคล ในกรณีนี้บริษัทต้องดำเนินการให้มั่นใจว่าบริษัทมีฐานในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (ข้อมูลสุขภาพ) อ้างอิง เช่น ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูลสุขภาพเหล่านั้น เพื่อพิจารณาประกอบการเข้ารับทำงานของบริษัท ทั้งนี้ บริษัทอาจขอความยินยอมโดยชัดแจ้ง สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวข้างต้นไว้ตั้งแต่ขั้นตอนที่เจ้าของข้อมูลส่วนบุคคลกรอกใบสมัคร หรือขั้นตอนก่อนส่งตัวเจ้าของข้อมูลส่วนบุคคลไปตรวจสอบสุขภาพยังโรงพยาบาล ก็ได้
- สำหรับการตรวจประวัติอาชญากรรม ปัจจุบันบริษัทสามารถทำการตรวจสอบได้กับสำนักงานตำรวจแห่งชาติ ซึ่งเป็นหน่วยงานที่มีอำนาจดูแล โดยที่สำนักงานตำรวจแห่งชาติได้มีการกำหนดแบบความยินยอมเป็นการเฉพาะอยู่แล้ว บริษัทอาจใช้แบบฟอร์มของสำนักงานตำรวจแห่งชาติ ประกอบขณะกรอกใบสมัครเข้าทำงาน เพื่อใช้ในการตรวจสอบประวัติอาชญากรรมกับสำนักงานตำรวจแห่งชาติได้ เว้นแต่มีการตรวจประวัติอาชญากรรมด้วยวิธีการอื่นด้วย

12.1.4 ช่วงระยะเวลาการจ้างงาน (Employee Lifecycle)

บริษัทอาจมีประเด็นที่ต้องพิจารณาดังนี้

1. การทำประกันภัยสุขภาพให้กับพนักงาน (Health Insurance)

ในการทำประกันภัยสุขภาพให้กับพนักงานซึ่งโดยมากจะเป็นการทำประกันภัยสุขภาพแบบกลุ่ม ซึ่งในกรณีนี้หากบริษัทเข้ามาเกี่ยวข้อง บริษัทจะต้องขอความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเพื่อการดำเนินการทำประกันกลุ่มให้กับพนักงานแต่ละคน โดยที่หาก

บริษัท ต้องการที่จะประมวลผลข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์อื่น เช่น ประมวลผลข้อมูลสุขภาพเพื่อประเมินความสามารถของพนักงาน บริษัทจะต้องระบุขอบเขตของความยินยอมโดยชัดแจ้งนั้นให้ชัดเจน

2. การสอบสวนในองค์กร (Internal Investigation)

ในกรณีที่บริษัทสันนิษฐานว่า พนักงานอาจกระทำความผิดวินัยหรือกฎหมาย เมื่อบริษัท จำเป็นจะต้องทำการสอบสวนและลงโทษทางวินัย และ/ หรือดำเนินคดีแล้ว บริษัทควรจะต้องดำเนินการต่าง ๆ ต่อไปนี้ เพื่อให้แน่ใจว่า มีการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมตามกฎหมาย

- กรณีมีการกระทำความผิดทางวินัยของบริษัท แต่ไม่ถึงขั้นเป็นความผิดอาญาที่ต้องดำเนินคดี - ในกรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไป เช่น การสัมภาษณ์ผู้รู้เห็น เหตุการณ์ หรือการสอบสวนพนักงานผู้รับผิดชอบ เช่นนี้ บริษัทอาจอ้างอิงฐานประโยชน์อันชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลเพื่อการตรวจสอบ หรือสอบสวนได้
- กรณีการกระทำผิดกฎหมายที่บริษัท จะต้องดำเนินคดีแพ่ง/ อาญา
 - สำหรับการประมวลผลข้อมูลส่วนบุคคลทั่วไป บริษัทสามารถอ้างอิงฐานประโยชน์อันชอบธรรมได้ เพราะเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อการก่อตั้ง หรือดำเนินการตามสิทธิเรียกร้องของบริษัท พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24
 - ส่วนการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 บริษัทอาจอ้างอิงฐานการก่อตั้ง ได้แย้ง และดำเนินการตามสิทธิเรียกร้องขอบริษัทได้ (ตามรายละเอียดที่ได้อธิบายไว้แล้ว ในบทที่ 5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล)

3. กรณีอื่น ๆ เช่น การดำเนินการการจ่าย เช่น เงินเดือน (Salary)

การประมวลผลข้อมูลส่วนบุคคลเพื่อการดำเนินการต่าง ๆ ตามสัญญา รวมถึงการจ่ายเงินเดือน สามารถอ้างอิงฐานสัญญาได้ เนื่องจากการประมวลผลดังกล่าวเป็นไปเพื่อการดำเนินการตามสิทธิ และหน้าที่ของบริษัทตามสัญญาที่มีกับพนักงาน

12.1.5 เมื่อสิ้นสุด/ ภายหลังการจ้างงาน (After Employment)

บริษัทอาจมีประเด็นที่ต้องพิจารณาดังนี้

เมื่อสิ้นสุดสัญญาจ้างแล้ว ไม่ว่าจะด้วยการลาออก หรือการเลิกจ้าง มักมีปัญหว่าบริษัทจะสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานดังกล่าวไว้ได้หรือไม่ เพราะไม่มีสัญญาจ้าง ซึ่งส่วนใหญ่จะถูกอ้างอิงเป็นฐานในการประมวลผลข้อมูลส่วนบุคคลในกรณีนี้ คำตอบคือ โดยหลัก บริษัทสามารถเก็บรักษาข้อมูลส่วนบุคคลของพนักงานเหล่านั้นอยู่เท่าที่มีความจำเป็น เช่น บริษัทอาจจำเป็นต้องเก็บรักษาข้อมูลเลขบัญชีธนาคารของพนักงานไว้ เพื่อดำเนินการจ่ายเงินจากกองทุนสำรองเลี้ยงชีพของพนักงาน เมื่อได้รับมาภายหลังพนักงานได้ลาออกไปทำงานที่อื่นแล้ว เป็นต้น

ข้อแนะนำ

- บริษัทควรดำเนินการตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของพนักงาน ที่ทำโดยฝ่ายทรัพยากรบุคคลของบริษัท ตั้งแต่ต้นจนจบกระบวนการจ้างงาน โดยบริษัทควรจะต้องระบุให้ได้ว่าในแต่ละกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคล บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดบ้าง ประมวลผลข้อมูลส่วนบุคคลไปเพื่อวัตถุประสงค์ใด และอ้างอิงฐานการประมวลผลข้อมูลส่วนบุคคลใด เพื่อให้แน่ใจว่าบริษัทได้ดำเนินการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนด
- บริษัทจะต้องระบุรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล พร้อมทั้งสิทธิของพนักงานในฐานะเจ้าของข้อมูลส่วนบุคคล ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของบริษัทเพื่อแจ้งให้พนักงานทุกคนทราบด้วย
- เมื่อมีการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของบริษัทแล้ว บริษัทจะต้องบันทึกข้อมูลส่วนบุคคลเหล่านั้นไว้ในแบบการบันทึกการประมวลผลข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และเพื่อการสะดวกต่อการตรวจสอบของหน่วยงานกำกับดูแล

12.2 แนวทางการดำเนินการในการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ข้อมูลส่วนบุคคล¹¹³

****รายละเอียดเกี่ยวกับแนวทางในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลต่อไปนี้เป็นเพียงตัวอย่างที่แนวปฏิบัตินี้นำเสนอ ซึ่งอาจจะต้องมีการแก้ไขเปลี่ยนแปลง เมื่อคณะกรรมการมีการประกาศกำหนดหลักเกณฑ์ดังกล่าว****

ตามที่ได้อธิบายไว้แล้วเบื้องต้น เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 33 เพียงแต่กำหนดให้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอใช้สิทธิในการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ โดยการร้องขอใช้สิทธิดังกล่าวแบ่งออกได้เป็น 3 กรณีดังต่อไปนี้

- การขอให้ลบ
- การขอให้ทำลาย
- การขอให้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

หลักเกณฑ์ และข้อกำหนดเกี่ยวกับการลบ การทำลาย หรือการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นให้เป็นไปตามกฎหมายลำดับรอง

อย่างไรก็ดี ระหว่างที่ยังไม่มีกฎหมายลำดับรองในเรื่องที่เกี่ยวข้องกับการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ แนวทางปฏิบัตินี้ขอแนะนำเสนอแนวทางในการลบ การทำลาย หรือการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลต่อสมาคม องค์กรวิชาชีพ และบริษัท เพื่อให้นำไปพิจารณาและปรับใช้เป็นแนวทางเดียวกันของภาคธุรกิจ องค์กรวิชาชีพ โดยมียละเอียดดังนี้

หลักการ: “การเก็บรักษาข้อมูลส่วนบุคคลนั้นจะต้องเก็บไว้เท่าที่มีความจำเป็นในการประมวลผลข้อมูลเพื่อให้บรรลุวัตถุประสงค์เท่านั้น”

สำหรับแนวทางปฏิบัติในส่วนนี้ จะมุ่งเน้นการอธิบายเกี่ยวกับแนวทางในการลบ การทำลาย หรือการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล (“การลบข้อมูลส่วนบุคคล”) ที่ถูกเก็บอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เป็นหลัก

¹¹³ https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

ซึ่งสำหรับการลบข้อมูลส่วนบุคคลที่ถูกเก็บอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น เป็นที่เข้าใจกันดีว่าไม่สามารถลบหรือทำลายได้ง่าย เพราะการส่งย้ายข้อมูลอิเล็กทรอนิกส์ดังกล่าวไปยังไฟล์ขยะ (Recycle Bin) นั้นเป็นเพียงแค่การย้ายที่เก็บรักษาข้อมูล (Archiving) โดยที่ยังสามารถเรียกข้อมูลดังกล่าวกลับมาใช้งานใหม่ (Re-instated) หรือกู้คืน (Retrieving) ได้ ดังนั้น ข้อมูลส่วนบุคคลถูกย้ายไปเก็บในไฟล์ขยะและยังสามารถนำกลับมาใช้ได้จึงยังถือได้ว่า ยังเป็นข้อมูลส่วนบุคคลที่ยังไม่ถูกดำเนินการลบข้อมูลส่วนบุคคลและยังคงได้รับการคุ้มครองตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่าง สถานการณ์เกี่ยวกับการลบข้อมูลส่วนบุคคล

- ข้อมูลอิเล็กทรอนิกส์นั้นถูกลบด้วยเจตนาของผู้ควบคุมข้อมูลส่วนบุคคลที่จะไม่ใช้หรือไม่เข้าถึงข้อมูลดังกล่าวอีก แต่ข้อมูลดังกล่าวอาจยังมีตัวตนอยู่ในรูปแบบของกระแสอิเล็กทรอนิกส์ (Electronic Ether) เช่น กระแสอิเล็กทรอนิกส์ที่รอการถูกเขียนข้อมูลทับ
- กรณีที่นำข้อมูลส่วนบุคคลบนเอกสารไปผ่านการตัดกระดาษในเครื่องทำลายเอกสาร ซึ่งแม้ว่าจะสามารถนำกระดาษที่ถูกตัดทำลายนั้นกลับมาต่อกันใหม่เพื่อประกอบเป็นข้อมูลส่วนบุคคลก็ได้ แต่ก็เป็นกรณีที่เป็นไปได้อย่างที่บริษัทจะนำข้อมูลดังกล่าวกลับมาต่อใหม่ กล่าวคือ เป็นการทำลายข้อมูลส่วนบุคคลไปโดยไม่มีเจตนาที่จะนำกลับมาใช้นั่นเอง
- ข้อมูลอิเล็กทรอนิกส์ที่ควรจะต้องถูกลบแต่ในความเป็นจริงแล้วข้อมูลดังกล่าวยังอยู่ในระบบเพราะเหตุผลทางเทคนิคที่ไม่สามารถลบข้อมูลดังกล่าวได้โดยไม่ลบข้อมูลอื่นที่อยู่ในกลุ่มก้อนเดียวกัน กรณีนี้อาจเกิดขึ้นได้ในกรณีที่ศาลมีคำสั่งให้ลบข้อมูลส่วนบุคคล

ด้วยเหตุนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหราชอาณาจักร (Information Commission Office: ICO) ก็เข้าใจถึงความยากลำบากในการลบข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ดังกล่าว ICO จึงกำหนดหลักการ “Beyond Use” มาปรับใช้กับการลบข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ กล่าวคือ แม้ว่าการลบข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์อาจจะทำไม่ได้อย่างเสถียรเด็ดขาดเหมือนกับการทำลายข้อมูลที่อยู่ในรูปแบบเอกสาร เช่น การเผาทำลาย ก็ตาม แต่ ICO ก็เชื่อว่าได้มีการลบข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ดังกล่าวแล้ว หากมีการทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในสถานะ “Put Beyond Use” โดยแม้ไม่มีการลบข้อมูลเด็ดขาด ก็เชื่อได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลได้มีการลบ หรือทำลายข้อมูลส่วนบุคคลแล้ว ซึ่งการ “Put Beyond Use” นั้น มีตัวอย่างดังนี้

- ไม่สามารถ หรือไม่พยายาม ที่จะใช้ข้อมูลส่วนบุคคลนั้นในการประกอบการตัดสินใจเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล หรือที่จะใช้ข้อมูลส่วนบุคคลนั้นไปในทางใดที่จะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทางใด ๆ

- ไม่ให้องค์กรอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลนั้นได้
- แวดล้อมข้อมูลส่วนบุคคลนั้นด้วยมาตรการความมั่นคงทางเทคนิคและทางองค์กรที่เหมาะสม และ
- ทำการลบข้อมูลส่วนบุคคลนั้นอย่างเด็ดขาดเมื่อทำได้ (ดูตัวอย่างด้านล่าง)

ตัวอย่างการลบข้อมูลส่วนบุคคล¹¹⁴

- การทำลายในทางกายภาพ (Physical Destruction) คือ การทำลายอุปกรณ์ที่เกี่ยวข้องในทางกายภาพที่เกี่ยวข้องเพื่อไม่ให้นำอุปกรณ์กลับมาใช้ได้
- การลบอย่างปลอดภัยโดยใช้โปรแกรม (Secure Deletion Software) คือ การใช้โปรแกรมเพื่อเขียนข้อมูลทับลงไปบนระบบ ซึ่งอาจทำมากกว่าหนึ่งครั้งก็ได้
- การย้อนกลับสู่การตั้งค่าแบบโรงงาน (Restore to Factory Setting) คือ อุปกรณ์บางประเภทอาจมีฟังก์ชันในการเลือกที่จะให้มี “การย้อนกลับสู่การตั้งค่าแบบโรงงาน” ซึ่งจะทำให้การตั้งค่าสถานะต่าง ๆ ของอุปกรณ์นั้นย้อนกลับไปสู่สถานะที่เพิ่งถูกซื้อ
- การส่งให้ผู้เชี่ยวชาญ (Send to a Specialist) คือ การให้ผู้เชี่ยวชาญดำเนินการลบข้อมูลแทน
- การตั้งค่าใหม่ (Formatting) คือ การตั้งค่าอุปกรณ์โดยการสร้างโครงสร้างข้อมูลและระบบไฟล์ขึ้นมาใหม่

ข้อสังเกต

- การลบข้อมูล คือ กรณีที่ข้อมูลถูกนำออกและไม่สามารถเห็นหรือกู้คืนมาได้โดยง่าย เช่น การย้ายข้อมูลไปยังไฟล์ขยะ (Recycle Bin) และทำการ ‘Quick Format’ อุปกรณ์เก็บข้อมูลนั้น หรือตั้งค่าให้ย้อนกลับไปที่การตั้งค่าแบบโรงงาน เช่นนี้อาจถือได้ว่าเป็นการลบข้อมูลแล้ว แม้ว่าข้อมูลดังกล่าวอาจจะสามารถกู้คืนกลับมาโดยผู้เชี่ยวชาญก็ตาม
- การทำลายข้อมูล คือ กรณีที่ข้อมูลถูกถอดออกจากอุปกรณ์และไม่สามารถกู้คืนข้อมูลนั้นกลับมาได้ แม้ว่าจะให้ผู้เชี่ยวชาญเป็นผู้กู้ข้อมูลก็ตาม เช่น การทำลายทางกายภาพ หรือการส่งให้ผู้เชี่ยวชาญเป็นต้น

¹¹⁴ <https://ico.org.uk/your-data-matters/online/deleting-your-data-from-computers-laptops-and-other-devices/>

- การจัดทำข้อมูลนิรนาม (Anonymization) กับ การแฝงข้อมูล (Pseudonymization) อาจถือได้ว่าเป็นอีกหนึ่งแนวทางในการลบข้อมูลส่วนบุคคล ทั้งนี้ ให้เป็นไปตามหลักเกณฑ์ที่เกี่ยวข้องตามกฎหมายลำดับรอง
- สำหรับการลบข้อมูลส่วนบุคคลที่ถูกเก็บอยู่ในรูปแบบอื่น เช่น เอกสาร เป็นต้น บริษัทอาจใช้วิธีการลบข้อมูลส่วนบุคคลที่มีการใช้อยู่ทั่วไป เช่น การขีดฆ่าด้วยหมึกดำที่ไม่สามารถลบได้ การนำเอกสารไปตัดทำลาย หรือการนำเอกสารไปเผาทำลาย

12.3 ตัวอย่างข้อมูลส่วนบุคคล และฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สรุปฐานในการประมวลผลข้อมูลส่วนบุคคล				
วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป (มาตรา 24)	ฐานการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (มาตรา 26)	ตัวอย่างข้อมูลส่วนบุคคล
การเสนอขาย (กรณีที่บริษัทเป็นผู้ติดต่อก่อน เช่น Telemarketing)	ผู้มุ่งหวัง	ความยินยอม	ความยินยอมโดยชัดแจ้ง	ชื่อ-นามสกุล ที่อยู่ อาชีพ ข้อมูลการเงิน ข้อมูลสุขภาพ
การเสนอขาย (กรณีที่ผู้มุ่งหวังติดต่อมาก่อน)	ผู้มุ่งหวัง	สัญญา	ประโยชน์สาธารณะที่สำคัญ	ที่อยู่ อาชีพ ข้อมูลการเงิน ข้อมูลสุขภาพ ข้อมูลการใช้เว็บไซต์ของบริษัทหรือของเว็บไซต์อื่น
การเสนอขายผลิตภัณฑ์ของบริษัทให้ลูกค้าเดิมเพิ่มเติม เช่น ผู้เอาประกันภัยซื้อกรมธรรม์รถยนต์แล้ว บริษัท จะเสนอขายประกันภัยอุบัติเหตุส่วนบุคคลเพิ่มเติม	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ข้อมูลการเงิน ข้อมูลสุขภาพ ข้อมูลการใช้สิทธิภายใต้กรมธรรม์ ข้อมูลการใช้เว็บไซต์ของบริษัทหรือของเว็บไซต์อื่น
การเสนอขายผลิตภัณฑ์ของบริษัทในเครือหรือพันธมิตรของธุรกิจ โดยมีลักษณะที่อยู่ในความคาดหมายของลูกค้า	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ข้อมูลการเงิน ข้อมูลสุขภาพ ข้อมูลการใช้เว็บไซต์ของบริษัทหรือของเว็บไซต์อื่น

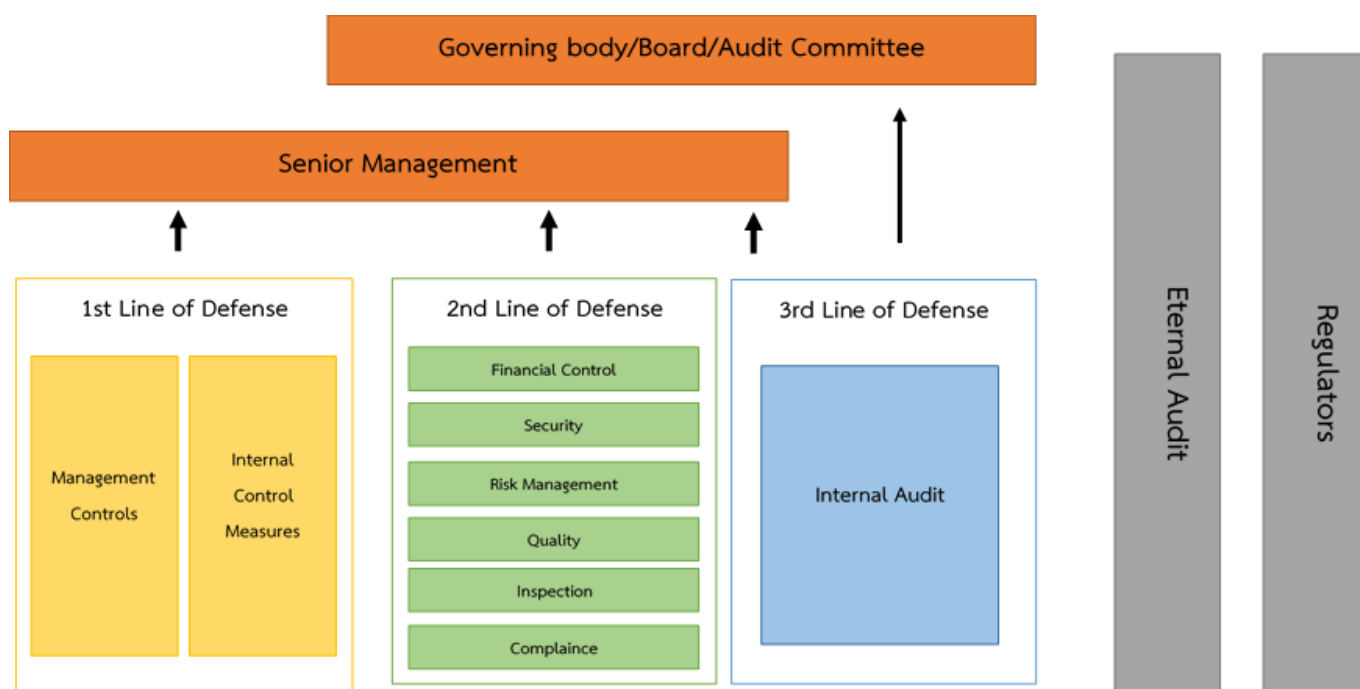
สรุปฐานในการประมวลผลข้อมูลส่วนบุคคล				
วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป (มาตรา 24)	ฐานการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (มาตรา 26)	ตัวอย่างข้อมูลส่วนบุคคล
การเข้าทำสัญญาประกัน การพิจารณารับประกัน	ผู้เอาประกันภัย	สัญญา	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ที่อยู่ อายุ อาชีพ ข้อมูลสำหรับติดต่อ ข้อมูลการเงิน ข้อมูลสุขภาพ ข้อมูลทางทะเบียน ใบอนุญาตขับขี่รถยนต์
	ผู้รับประกัน	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ที่อยู่ อายุ ข้อมูลสำหรับติดต่อ
	ผู้ชำระเงิน	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	
	บุคคลอื่น ๆ ในครอบครัว	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	
การพิสูจน์ยืนยันตัวตน	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม/ หน้าที่ตามกฎหมาย	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล เลขประจำตัวบัตรประชาชน
การพิจารณาและการจ่ายค่าสินไหมทดแทน	ผู้เอาประกันภัย	สัญญา	สิทธิเรียกร้อง (Legal Claims)	ชื่อ-นามสกุล เลขประจำตัวบัตรประชาชน เลขบัญชี ข้อมูลสุขภาพ ข้อมูลการเดินทาง ข้อมูลทางทะเบียน ใบอนุญาตขับขี่รถยนต์
การส่งรายงานให้กับสำนักงาน คปภ.	ผู้เอาประกันภัย	หน้าที่ตามกฎหมาย	หน้าที่ตามกฎหมาย	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย
การเอาประกันภัยต่อ	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย

สรุปฐานในการประมวลผลข้อมูลส่วนบุคคล				
วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป (มาตรา 24)	ฐานการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (มาตรา 26)	ตัวอย่างข้อมูลส่วนบุคคล
การเรียกร้องค่าสินไหมทดแทนตามสัญญาประกันภัยต่อ	ผู้เอาประกันภัย	สัญญา	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย ข้อมูลสุขภาพ ข้อมูลการเดินทาง ข้อมูลทางทะเบียน
เพื่อการป้องกันการฉ้อโกง (รวมถึงการเปิดเผยข้อมูลภายในภาคธุรกิจ)	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ประวัติอาชญากรรม
การปฏิบัติตามกฎหมายหรือคำสั่งอื่น ๆ	ผู้เอาประกันภัย	หน้าที่ตามกฎหมาย	หน้าที่ตามกฎหมาย	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย
การดำเนินการทางกฎหมาย การดำเนินการเกี่ยวกับสิทธิเรียกร้อง	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	สิทธิเรียกร้อง (Legal Claims)	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย ข้อมูลทางทะเบียน
การซื้อ/ขาย กิจการ หรือการปรับโครงสร้างองค์กร	ผู้เอาประกันภัย	ประโยชน์อันชอบธรรม	ประโยชน์สาธารณะที่สำคัญ	ชื่อ-นามสกุล ข้อมูลเกี่ยวกับกรรมธรรม์ประกันภัย
	ผู้รับประโยชน์			ชื่อ-นามสกุล ที่อยู่ อายุ ข้อมูลสำหรับติดต่อ
	ผู้ชำระเงิน			
	บุคคลอื่น ๆ ในครอบครัว			

12.4 แนวปฏิบัติเกี่ยวกับ Three Lines of Defense สำหรับการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ในการประกอบธุรกิจต่าง ๆ โดยเฉพาะการประกอบธุรกิจประกันวินาศภัยของบริษัท ย่อมมีความเสี่ยง (Risks) ในหลาย ๆ ด้าน ไม่ว่าจะเป็นด้านการตลาด ด้านกลยุทธ์ ด้านการปฏิบัติการ ด้านเทคโนโลยีสารสนเทศของบริษัท และด้านการประกันภัย ที่บริษัทต้องกำกับและบริหารจัดการกับความเสี่ยงเหล่านั้น และนอกจากความเสี่ยงด้านต่าง ๆ ข้างต้นแล้ว ณ ปัจจุบัน ความเสี่ยงอีกด้านหนึ่งที่บริษัท จำต้องคำนึงถึงอย่างมากก็คือ ความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ในเรื่องการกำกับดูแลความเสี่ยง (Risk Governance) ของบริษัท บริษัท อาจมีการดำเนินการกำกับดูแลความเสี่ยงต่าง ๆ ข้างต้น ขององค์กรตนเองในรูปแบบที่แตกต่างกัน ซึ่งหนึ่งในรูปแบบหรือวิธีการที่อาจใช้ในการกำกับดูแลความเสี่ยงของบริษัท ก็คือรูปแบบที่เรียกว่า Three Lines of Defense ซึ่งมีลักษณะ หรือ



โครงสร้าง^{115 116} ดังนี้

¹¹⁵ FERMA's Views on the Guidelines on Data Protection Officers Adopted on 13 December 2016 by the Article 29 Data Protection Working Party <https://www.ferma.eu/app/uploads/2019/02/ferma-comments-dpo-guidelines-art-29-working-party.pdf>, เข้าถึงเมื่อวันที่ 6 มิถุนายน 2562

¹¹⁶ The Three Lines Of Defense In Effective Risk Management And Control, <https://na.theiaa.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>, เข้าถึงเมื่อวันที่ 6 มิถุนายน 2562

1st Line of Defense – เป็นส่วนที่มีหน้าที่โดยตรงในการจัดการและควบคุมความเสี่ยงของบริษัท ซึ่งได้แก่ส่วนงานที่รับผิดชอบการดำเนินธุรกิจในแต่ละวันของบริษัท กล่าวคือ Business Unit ต่าง ๆ

2nd Line of Defense – เป็นส่วนงานที่มีหน้าที่ประสานงาน สนับสนุน และควบคุมประสิทธิภาพของกรอบการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการบริหารและจัดการความเสี่ยงที่ดำเนินการโดย 1st Line เป็นไปอย่างถูกต้อง และเหมาะสม รวมถึงการกำกับดูแลให้บริษัทดำเนินการเพื่อให้เป็นไปตามกฎหมาย การกำหนดกรอบ หรือเป้าหมายในการดำเนินการเกี่ยวกับการบริหารความเสี่ยงให้กับบริษัท การให้คำแนะนำ หรือแนวทางในการดำเนินการบริหารความเสี่ยง

3rd Line of Defense – เป็นส่วนงานที่ทำหน้าที่ให้ความเชื่อมั่น และประเมินประสิทธิภาพในการบริหารความเสี่ยงของบริษัท (Risk Assurance)¹¹⁷ ซึ่งหน้าที่ของส่วนงานนี้คือการติดตาม ตรวจสอบ และประเมินผลการจัดการความเสี่ยง เพื่อรายงานให้แก่คณะกรรมการบริษัทได้ทราบ

ในส่วนของการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งมีกฎหมายเฉพาะเข้ามาเกี่ยวข้อง คือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ได้มีการกล่าวถึงบุคคลหนึ่งซึ่งมีความสำคัญกับองค์กร หรือบริษัท อย่างมาก ได้แก่ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หรือที่เรียกว่า Data Protection Officer (DPO) ซึ่งดังที่ได้กล่าวไปแล้วในเรื่องของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะเห็นได้ว่าหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดได้แก่

1) ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล แก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าว

2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าว เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

3) ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของบุคคลดังกล่าวในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹¹⁷ คปก., การบริหารความเสี่ยงสำหรับบุคคล, <http://www.oic.or.th/sites/default/files/content/85938/bth6.pdf>, เข้าถึงเมื่อวันที่ 6 มิถุนายน 2562

จากหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลข้างต้น จะเห็นได้ว่าหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดนั้น เป็นหน้าที่ที่อยู่ในขอบข่ายของ 2nd Line of Defense กล่าวคือ มีหน้าที่ให้คำแนะนำในการปฏิบัติตามกฎหมาย ตรวจสอบการดำเนินงาน ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น คณะกรรมการ หรือสำนักงาน ดังนั้น เพื่อการกำกับดูแลความเสี่ยงในด้านที่เกี่ยวข้องกับข้อมูลส่วนบุคคล บริษัทควรจัดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทอยู่ในส่วนของ 2nd Line of Defense

12.5 แนวทางปฏิบัติเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

12.5.1 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) คืออะไร

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) คือ กระบวนการที่ถูกกำหนดให้มีการจัดทำขึ้นเพื่อประเมินผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่การประมวลผลข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล (likely to result in a high risk to the rights and freedoms of natural persons) ตาม GDPR¹¹⁸ ทั้งนี้ คำว่า “สิทธิและเสรีภาพของบุคคล” นั้นนอกจากจะหมายถึงสิทธิในความเป็นส่วนตัวแล้ว ยังควรมีความหมายรวมไปถึงสิทธิและเสรีภาพขั้นพื้นฐานที่รับรองไว้ในรัฐธรรมนูญอีกด้วย

ในปัจจุบัน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ยังไม่ได้มีบทบัญญัติกำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่จะต้องจัดทำ DPIA ไว้โดยตรงเหมือน GDPR แต่มีการกำหนดไว้ในประกาศสำนักงาน คปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้ำสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564 เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเช่นเดียวหรือเทียบเท่ากับ GDPR คณะกรรมการอาจขยายความคำว่า “มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 37 (1) และมาตรา 40 (2) ให้รวมถึงการจัดทำ DPIA เป็นส่วนหนึ่งของมาตรการข้างต้นด้วยก็ได้

ทั้งนี้ หากบริษัทมีความประสงค์ที่จะจัดทำ DPIA เพื่อให้บริษัทมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่า GDPR บริษัทสามารถยึดถือตามแนวปฏิบัติ¹¹⁹ของคณะทำงานเกี่ยวกับการคุ้มครองข้อมูล (Data Protection Working Party: WP29) ที่ถูกจัดตั้งขึ้นตามกฎหมายของสหภาพยุโรป¹²⁰ ได้

12.5.2 การประมวลผลข้อมูลส่วนบุคคลที่ควรจัดให้มีการทำ DPIA

ตามแนวปฏิบัติเกี่ยวกับการจัดทำ DPIA ตามที่ Data Protection Working Party (WP29) กำหนด ได้มีการอธิบายและแนะนำให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำ DPIA เมื่อมีการประมวลผลข้อมูลส่วนบุคคลเข้าข่ายหรือมีคุณลักษณะที่ตรงกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้ ซึ่งโดยหลักผู้ควบคุมข้อมูล

¹¹⁸ Article 35 Paragraph 1 of the GDPR

¹¹⁹ Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, (17/EN, WP 248 rev.01), Adopted on 4 April 2017 as last Revised and Adopted on 4 October 2017

¹²⁰ Article 29 of Directive 95/46/EC. Data Protection Working Party ที่เป็นองค์กรอิสระที่มีหน้าที่ในการให้คำปรึกษาเกี่ยวกับการคุ้มครองข้อมูลและความเป็นส่วนตัวในสหภาพยุโรป

ส่วนบุคคลควรจัดทำ DPIA เมื่อมีการดำเนินกิจกรรมการประมวลผลตามที่ยกตัวอย่างด้านล่าง 2 กิจกรรมขึ้นไป

- (1) การประเมินหรือการให้คะแนน (Evaluation or Scoring) ซึ่งรวมไปถึงการจัดทำโปรไฟล์ (Profiling) และการคาดการณ์ (Predicting) โดยเฉพาะกรณีเกี่ยวกับความสามารถในการทำงาน สถานทางเศรษฐกิจ สุขภาพ รสนิยมหรือความสนใจ ความน่าเชื่อถือหรือพฤติกรรม สถานที่หรือการเคลื่อนไหวของเจ้าของข้อมูลส่วนบุคคล เช่น บริษัททำการตรวจสอบประวัติของผู้เอาประกันภัยจากฐานข้อมูลการฉ้อโกงหรือฐานข้อมูลเครดิตหรือฐานข้อมูลการฟอกเงิน หรือบริษัทที่ประมวลผลข้อมูลโดยจัดทำโปรไฟล์ของลูกค้าที่เข้ามาใช้เว็บไซต์เปรียบเทียบผลิตภัณฑ์ประกันภัย (aggregator)
- (2) กระบวนการตัดสินใจอัตโนมัติที่ทำให้เกิดผลผูกพันทางกฎหมายหรือส่งผลที่มีนัยสำคัญในทางเดียวกัน (Automated-Decision Making with Legal or Similar Significant Effect) เช่น การประมวลผลข้อมูลที่จะนำไปสู่การกีดกันหรือเลือกปฏิบัติต่อบุคคล อย่างไรก็ตามหากการประมวลผลข้อมูลซึ่งผลกระทบต่อบุคคลน้อยมากถึงไม่มีผลกระทบจะไม่ถือว่าเป็นหลักเกณฑ์นี้
- (3) การเฝ้าระวังอย่างเป็นระบบ (Systematic Monitoring) เป็นกรณีที่มีการประมวลผลข้อมูลถูกใช้เพื่อเฝ้าสังเกต เฝ้าระวัง หรือควบคุมเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมไปถึงการเก็บรวบรวมข้อมูลผ่านระบบเครือข่าย หรือการเฝ้าระวังอย่างเป็นระบบในพื้นที่สาธารณะ¹²¹ การเฝ้าระวังในลักษณะนี้ถูกกำหนดให้เป็นหนึ่งในหลักเกณฑ์จัดทำ DPIA ด้วยเหตุผลว่าข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวมในสถานการณ์ที่เจ้าของข้อมูลส่วนบุคคลอาจไม่รู้ว่าเป็นผู้เก็บรวบรวมและจะนำไปใช้อย่างไร นอกจากนี้บุคคลอาจไม่สามารถหลีกเลี่ยงการประมวลผลข้อมูลจากพื้นที่สาธารณะดังกล่าวได้
- (4) ข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือข้อมูลโดยสภาพเป็นเรื่องส่วนบุคคลมาก (Sensitive Data or Data of a Highly Personal Nature) สำหรับข้อมูลที่มีความอ่อนไหว พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล¹²² และ GDPR¹²³ กำหนดประเภทข้อมูลส่วนบุคคลดังกล่าวไว้คล้ายคลึงกัน ซึ่ง

¹²¹ Article 35(3)(c) of the GDPR “a systematic monitoring of a publicly accessible area on a large scale”. The WP29 interprets “systematic” as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):

- occurring according to a system;
- pre-arranged, organized or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

¹²² มาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

¹²³ Article 9 and Article 10 of the GDPR

ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับความเห็นทางการเมือง ข้อมูลสุขภาพ ข้อมูลชีวภาพ และประวัติอาชญากรรม เป็นต้น เช่น บริษัททำการประมวลผลประวัติการรักษาพยาบาลของผู้เอาประกันภัย อุบัติเหตุเพื่อพิจารณาการจ่ายค่าสินไหมทดแทน นอกเหนือจากข้อมูลส่วนบุคคลที่มีความอ่อนไหวข้างต้นแล้ว WP29 ยังมีความเห็นเพิ่มเติมต่อไปอีกว่า การประมวลผลข้อมูลส่วนบุคคลที่โดยสภาพเป็นเรื่องส่วนบุคคลมาก ก็ถือว่าอยู่ในขอบเขตของหลักเกณฑ์ข้อนี้ด้วย กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลประเภทนี้อาจเพิ่มความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ด้วยเหตุที่ข้อมูลเหล่านี้เชื่อมโยงถึงกิจกรรมส่วนตัวหรืออาจส่งผลกระทบต่อการใช้สิทธิขั้นพื้นฐานหรืออาจส่งผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคลเมื่อมีการละเมิดข้อมูล เช่น การประมวลผลข้อมูลตำแหน่งที่อยู่ที่อาจมีการเก็บรวบรวมเพื่อนำมาคำนวณค่าเบี้ยประกันภัยรถยนต์ที่อาจมีผลกระทบต่อเสรีภาพในการเดินทางและเลือกถิ่นที่อยู่¹²⁴ หรือข้อมูลทางการเงินที่บริษัทเก็บรักษาไว้ (หมายเลขบัตรเครดิต) อาจถูกนำไปใช้กระทำความผิดได้ หากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ทั้งนี้ ในส่วนของข้อมูลส่วนบุคคลข้างต้นที่นอกเหนือจากข้อมูลส่วนบุคคลที่กฎหมายกำหนดให้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ ข้อเท็จจริงเกี่ยวกับความแพร่หลายของข้อมูลดังกล่าวในพื้นที่สาธารณะ (ทำโดยเจ้าของข้อมูลส่วนบุคคลหรือบุคคลที่สาม) ที่เจ้าของข้อมูลส่วนบุคคลคาดหมายได้ว่าอาจถูกนำไปใช้เพื่อวัตถุประสงค์อื่น ๆ อาจจะสามารถนำมาพิจารณาเป็นปัจจัยในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลได้เช่นกัน

(5) ประมวลผลข้อมูลในปริมาณมาก (Data Processed on a Large Scale) ในกรณีนี้ GDPR ไม่ได้ให้คำนิยามไว้อย่างไรถึงจะถือว่าเป็นปริมาณมาก อย่างไรก็ตาม WP29 แนะนำให้พิจารณาปัจจัยดังต่อไปนี้ เพื่อตัดสินว่าการประมวลผลข้อมูลนั้นอยู่ในปริมาณที่มากหรือไม่¹²⁵

- ก. จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง โดยที่อาจจะเป็นจำนวนเฉพาะเจาะจงหรือสัดส่วนโดยรวมอย่างใดอย่างหนึ่ง
- ข. ปริมาณของข้อมูล และ/หรือขอบเขตของข้อมูลต่าง ๆ ที่ถูกประมวลผล
- ค. ระยะเวลา หรือการคงอยู่ของกิจกรรมในการประมวลผลข้อมูล
- ง. ขอบเขตทางภูมิศาสตร์ของการประมวลผลข้อมูล

(6) การจับคู่หรือรวมชุดข้อมูล (Matching or Combining Datasets) เช่น กรณีการจับคู่หรือรวมชุดข้อมูลที่เกิดจากกระบวนการประมวลผลข้อมูล ตั้งแต่ 2 กระบวนการขึ้นไป ซึ่งกระบวนการ

¹²⁴ มาตรา 38 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

¹²⁵ Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), (16/EN, WP 243 rev.01),

Adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017

ดังกล่าวอาจจะแตกต่างกันที่วัตถุประสงค์ในการประมวลผลข้อมูล และ/หรือที่มีผู้ควบคุมข้อมูลส่วนบุคคลเป็นคนละคน โดยที่เป็นการตีความความหมายตามสมควรของเจ้าของข้อมูลส่วนบุคคล

(7) ข้อมูลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลที่เป็นบุคคลเปราะบาง (Data Concerning Vulnerable Data Subjects)¹²⁶ เนื่องจากมีความไม่เท่าเทียมทางอำนาจระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล กล่าวคือ บุคคลบางกลุ่มอาจจะไม่สามารถให้ความยินยอมหรือโต้แย้งการประมวลผลข้อมูลส่วนบุคคลหรือการใช้สิทธิของตนได้โดยง่าย ซึ่งเจ้าของข้อมูลส่วนบุคคลที่เป็นบุคคลเปราะบางนั้นอาจรวมถึง ผู้เยาว์ ลูกจ้าง คนพิการ จิต ผู้ลี้ภัย คนชรา ผู้ป่วย เป็นต้น หรือกรณีใด ๆ ที่สามารถระบุความไม่เท่าเทียมกันในทางความสัมพันธ์ระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(8) การประยุกต์ใช้ หรือการใช้เทคโนโลยีใหม่ หรือมาตรการทางองค์กร (Innovative Use or Applying New Technological or Organizational Solutions) GDPR¹²⁷ อธิบาย การใช้เทคโนโลยีใหม่ ในลักษณะที่ “เป็นไปตามระดับความรู้เกี่ยวกับเทคโนโลยีที่มีอยู่แล้ว” (Accordance with The Achieved State of Technological Knowledge) ดังนั้น เมื่อมีการใช้เทคโนโลยีใหม่ ก็ย่อมจะต้องจัดทำ DPIA ประกอบด้วย เนื่องจาก DPIA จะช่วยให้ผู้จัดทำเข้าใจและบริหารความเสี่ยงอันอาจเกิดจากการใช้เทคโนโลยีใหม่ที่ยังไม่มีใครรู้ได้แน่นอนว่าจะมีผลกระทบต่อสิทธิและเสรีภาพเท่าใด เช่น การใช้แอปพลิเคชัน IoT (Internet of Things) บางประเภทอาจมีผลกระทบอย่างมีนัยสำคัญแก่ชีวิตประจำวันและความเป็นส่วนตัวของบุคคล

(9) การประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลถูกกีดกันไม่ให้ใช้สิทธิหรือการใช้บริการ หรือสัญญา (Processing Operations that Prevents Data Subjects From Exercising a Right or Using a Service or a Contract)¹²⁸ คือการประมวลผลข้อมูลส่วนบุคคลที่มุ่งให้เกิดเปลี่ยนแปลง หรือปฏิเสธการเข้าถึงการบริการหรือการเข้าทำสัญญา เช่น ธนาคารตรวจสอบข้อมูลเครดิตของลูกค้าเพื่อตัดสินใจว่าจะให้กู้เงินหรือไม่ หรือบริษัทตรวจสอบประวัติสุขภาพของผู้มุ่งหวังเพื่อพิจารณารับหรือไม่รับประกันภัย

การจัดทำ DPIA ในครั้งหนึ่งนั้นอาจจัดทำให้ครอบคลุมไปถึงการประมวลผลข้อมูลส่วนบุคคลที่มีกิจกรรม หรือลักษณะการประมวลผลที่คล้ายกันได้ เช่น ผู้ให้บริการรถไฟฟ้าอาจจะจัดทำ DPIA ฉบับเดียวสำหรับระบบกล้องวงจรปิด (CCTV) ของทุกสถานีรถไฟฟ้าที่อยู่ในความดูแลของผู้ให้บริการ เป็นต้น

¹²⁶ Recital 75 of the GDPR

¹²⁷ Article 35(1) and recitals 89 and 91 of the GDPR

¹²⁸ Article 22 and recital 91 of the GDPR

ตัวอย่างการพิจารณาจัดทำ DPIA

ตัวอย่างการประมวลผลข้อมูลส่วนบุคคล	หลักเกณฑ์ที่อาจเกี่ยวข้อง	เข้าข่ายจะต้องจัดทำ DPIA หรือไม่
การจัดทำประวัติการร้องเรียน ประกันภัย	- การประเมินหรือการให้คะแนน (Evaluation or Scoring) - ประมวลผลข้อมูลในปริมาณมาก (Data Processed on a Large Scale) - ข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือข้อมูลที่โดยสภาพเป็นเรื่องส่วนบุคคลมาก (Sensitive Data or Data of a Highly Personal Nature) - การจับคู่หรือรวมชุดข้อมูล (Matching or Combining Datasets)	เข้าข่าย
บริษัททำการเฝ้าดูพฤติกรรมของ ลูกจ้างอย่างเป็นระบบ ซึ่งรวมถึง การเฝ้าดูโต๊ะทำงานของลูกจ้าง การใช้งานอินเทอร์เน็ต ฯลฯ	- การเฝ้าระวังอย่างเป็นระบบ (Systematic Monitoring) - ข้อมูลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลที่เป็นบุคคลเปราะบาง (Data Concerning Vulnerable Data Subjects)	เข้าข่าย
บริษัทใช้รายชื่อ อีเมลหรือ หมายเลขโทรศัพท์ของผู้เอา ประกันภัยเพื่อส่งโปรโมชั่นส่งเสริม การขายแก่ผู้ที่สนใจ	- ประมวลผลข้อมูลในปริมาณมาก (Data Processed on a Large Scale)	ไม่เข้าข่าย (เนื่องจากการ ประมวลผลข้อมูลส่วน บุคคลที่มีลักษณะที่ควร จัดให้มี DPIA เพียง กิจกรรมเดียว)
Aggregator ที่จัดการให้เว็บไซต์ แสดงโปรโมชั่นส่งเสริมการขาย หรือโฆษณาสำหรับกรมธรรม์ ประกันภัย โดยที่ใช้วิธีจัดทำโปร ไฟล์ของผู้ใช้งานเว็บไซต์ซึ่งจำกัด อยู่เพียงรายการที่เคยมีการเรียกดู	- การประเมินหรือการให้คะแนน (Evaluation or Scoring)	ไม่เข้าข่าย (เนื่องจากการ ประมวลผลข้อมูลส่วน บุคคลที่มีลักษณะที่ควร จัดให้มี DPIA เพียง กิจกรรมเดียว)

ตัวอย่างการประมวลผลข้อมูล ส่วนบุคคล	หลักเกณฑ์ที่อาจเกี่ยวข้อง	เข้าข่ายจะต้องจัดทำ DPIA หรือไม่
หรือรายการที่เคยมีการซื้อใน เว็บไซต์ของตุนเท่านั้น		

อย่างไรก็ดี ถึงแม้ว่าการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลจะเข้าข่ายที่ควรจะต้องจัดทำ DPIA แต่หากผู้ควบคุมข้อมูลส่วนบุคคลตัดสินใจที่จะไม่จัดทำ DPIA เพื่อประเมินและจัดการความเสี่ยงแล้ว ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลควรจัดทำบันทึกถึงเหตุผลที่ไม่จัดทำ DPIA ดังกล่าว ซึ่งรวมถึงความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้เป็นหลักฐานด้วย

12.5.3 รายละเอียดและขั้นตอนการจัดทำ DPIA

DPIA ควรจะต้องจัดทำเมื่อใด?

บริษัทควรจะต้องจัดทำ DPIA ก่อนทำการประมวลผลข้อมูลส่วนบุคคล¹²⁹ เว้นแต่กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลนั้นได้มีมาอยู่ก่อนและได้รับการตรวจสอบจากหน่วยงานกำกับดูแลแล้ว เช่นนี้ บริษัทอาจจะต้องจัดทำ DPIA ก่อนการประมวลผลข้อมูลในกรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญเท่านั้น

การจัดทำ DPIA นั้น ควรจะเริ่มดำเนินการให้เร็วที่สุดเท่าที่จะเป็นไปได้ โดยที่บริษัทควรจะต้องคอยปรับปรุง DPIA ให้เป็นปัจจุบันที่สุด เพื่อแน่ใจว่ามีการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวพร้อมทั้งส่งเสริมมาตรการแก้ไขปัญหที่เป็นไปตามกฎหมายอีกด้วย ดังนั้น การจัดทำ DPIA จึงเป็นกระบวนการต่อเนื่องและไม่ใช้การทำครั้งเดียวแล้วจบ

บุคคลที่เกี่ยวข้องและมีหน้าที่ในการจัดทำ DPIA

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการให้แน่ใจว่าได้มีการจัดทำ DPIA¹³⁰ โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลนั้นอาจให้บุคคลอื่นจัดทำ DPIA ได้ แต่ความรับผิดชอบสำหรับการละเลยหน้าที่ดังกล่าวยังคงตกอยู่กับผู้ควบคุมข้อมูลส่วนบุคคลคนนั้นอยู่

ในกระบวนการจัดทำ DPIA นี้ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะต้องปรึกษาเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ด้วย¹³¹ โดยคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และการตัดสินใจของผู้

¹²⁹ Article 35(1) and 35(10), recitals 90 and 93 of the GDPR

¹³⁰ Article 35(2) of the GDPR

¹³¹ Article 35(2) of the GDPR

ควบคุมข้อมูลส่วนบุคคลนั้นจะต้องบันทึกรวมไปใน DPIA ด้วย ทั้งนี้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลยังควรที่จะต้องเฝ้าระวังการปฏิบัติตาม DPIA อีกด้วย¹³²

หากการประมวลผลข้อมูลส่วนบุคคลกระทำโดยผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าทั้งหมดหรือบางส่วน ผู้ประมวลผลข้อมูลส่วนบุคคลก็ควรที่จะต้องช่วยผู้ควบคุมข้อมูลส่วนบุคคลในการจัดทำ DPIA ด้วย โดยเป็นการช่วยเหลือในลักษณะของการให้ข้อมูลที่จำเป็น¹³³

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลก็ควรจะต้องสอบถามความเห็นของเจ้าของข้อมูลส่วนบุคคลหรือตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคคลที่เกี่ยวข้องในเรื่องเกี่ยวกับข้อกังวล มุมมอง หรือข้อความคิดเห็นเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามความเหมาะสมด้วย¹³⁴ ในส่วนของการสอบถามความเห็นนี้ WP29 มีความเห็นว่า สามารถทำได้หลากหลายวิธีการด้วยกัน โดยขึ้นกับพฤติการณ์ เช่น ทำการศึกษาทั่วไปเกี่ยวกับวิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล หรือส่งแบบสอบถามไปยังลูกค้ากลุ่มเป้าหมายในอนาคต เป็นต้น ทั้งนี้ มีข้อสังเกตว่าการสอบถามความเห็นของเจ้าของข้อมูลส่วนบุคคลหรือตัวแทนข้างต้นนี้ เป็นคนละส่วนกับการขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคล ต่อมาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลตัดสินใจแล้ว ผู้ควบคุมข้อมูลจะต้องบันทึกการตัดสินใจดำเนินการหรือไม่ดำเนินการพร้อมด้วยเหตุผล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตัดสินใจแตกต่างจากความเห็นของเจ้าของข้อมูลส่วนบุคคล

อนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลตัดสินใจที่จะไม่จัดทำ การสอบถามความเห็นของเจ้าของข้อมูลส่วนบุคคลหรือตัวแทนข้างต้นด้วยเหตุที่ว่าไม่เหมาะสมที่จะทำการสอบถาม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกเหตุที่ตนเห็นว่าไม่เหมาะสมเอาไว้ด้วย เช่น การทำการสอบถามความเห็นดังกล่าวจะทำให้สูญเสียความลับของแผนธุรกิจ หรือไม่ได้สัดส่วน หรือไม่สามารถกระทำได้ในทางปฏิบัติ

ท้ายที่สุด WP29 ได้แนะนำแนวทางปฏิบัติที่ดีเพิ่มเติม โดยที่แนะนำว่า ผู้ควบคุมข้อมูลส่วนบุคคลนั้นควรที่จะต้องทำการกำหนดนิยามหรือบันทึก หน้าที่หรือความรับผิดชอบอื่น ๆ ภายใต้นโยบายภายในของตน เช่น ในกรณีที่หน่วยธุรกิจใดอาจจะต้องจัดทำ DPIA ควรกำหนดให้ หน่วยธุรกิจดังกล่าวให้ข้อมูลและตรวจสอบความถูกต้องของ DPIA ฉบับนั้นด้วย หรือผู้ควบคุมข้อมูลส่วนบุคคลอาจขอความเห็นหรือคำปรึกษาจากผู้เชี่ยวชาญอิสระในแต่ละสาขาวิชาชีพได้ตามความเหมาะสม (ทนายความ ผู้เชี่ยวชาญระบบสารสนเทศ ผู้เชี่ยวชาญระบบความปลอดภัยของข้อมูล นักสังคมวิทยา ฯลฯ) หรือในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลให้ความช่วยเหลือในการทำ DPIA หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีนี้ก็สมควรที่จะต้องมีการกำหนดในรูปแบบของสัญญาโดยที่คำนึงถึงสภาพของการประมวลผลข้อมูลส่วนบุคคล และข้อมูลที่อยู่กับผู้ประมวลผลข้อมูลส่วนบุคคลประกอบด้วย¹³⁵ เป็นต้น

¹³² Article 39(1)(c) of the GDPR

¹³³ In line with Article 28(3)(f) of the GDPR

¹³⁴ Article 35(9) of the GDPR

¹³⁵ Article 28(3)(f) of the GDPR

ขั้นตอนในการจัดทำ DPIA¹³⁶

ขั้นที่ 1 ระบุเหตุจำเป็นในการจัดทำ DPIA

ขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับความจำเป็นที่จะต้องจัดทำ DPIA เนื่องจากในบางกรณีบริษัทอาจมีโครงการหรือแผนธุรกิจที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่มีการจัดทำ DPIA มาแล้ว ซึ่งหากโครงการ หรือกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่จะเริ่มดำเนินการใหม่นั้น ยังไม่มีการทำ DPIA บริษัทจะต้องพิจารณาหลักเกณฑ์ที่ได้อธิบายมาแล้วข้างต้นเพื่อพิจารณาว่าตนต้องดำเนินการจัดทำ DPIA หรือไม่

อย่างไรก็ตาม หากบริษัทพิจารณาและตัดสินใจที่จะไม่จัดทำ DPIA บริษัทควรจะต้องทำการบันทึกการตัดสินใจและเหตุผลสำหรับการตัดสินใจดังกล่าว รวมไปถึงคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย ทั้งนี้ หากบริษัทไม่แน่ใจว่าจะต้องจัดทำ DPIA หรือไม่ บริษัทควรจัดทำ DPIA เกี่ยวกับโครงการหรือแผนธุรกิจนั้น

ขั้นที่ 2 อธิบายกระบวนการประมวลผลข้อมูลส่วนบุคคล

อธิบายเกี่ยวกับวิธีการและเหตุผลในการใช้ข้อมูลส่วนบุคคลของบริษัท โดยที่คำอธิบายของบริษัทจะต้องประกอบด้วยหัวข้อดังต่อไปนี้

(1) ลักษณะของการประมวลผลข้อมูลส่วนบุคคล กล่าวคือ แผนของบริษัทที่มีต่อข้อมูลส่วนบุคคล ซึ่งรวมถึงตัวอย่างดังต่อไปนี้

- บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลอย่างไร
- บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลอย่างไร
- บริษัทจะใช้ข้อมูลส่วนบุคคลอย่างไร
- มีบุคคลใดบ้างที่สามารถเข้าถึงข้อมูลส่วนบุคคลนั้น
- บริษัทจะเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลใดบ้าง
- บริษัทจะใช้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่

¹³⁶ ICO, 'How do we do a DPIA?' < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how1> > (accessed 5 June 2020)

- ระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล
- มาตรการความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- บริษัทจะใช้เทคโนโลยีใหม่หรือไม่
- บริษัทจะมีการใช้วิธีการประมวลผลข้อมูลส่วนบุคคลแบบใหม่หรือไม่
- หลักเกณฑ์ใดที่บริษัทใช้ระบุความเสี่ยงสูงที่มีความเป็นไปได้

(2) ขอบเขตการประมวลผลข้อมูลส่วนบุคคล กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลของบริษัทจะครอบคลุมอะไรบ้าง ซึ่งรวมถึงตัวอย่างดังต่อไปนี้

- สภาพของข้อมูลส่วนบุคคล
- ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล
- ความอ่อนไหวของข้อมูลส่วนบุคคล
- ขอบข่ายและความถี่ในการประมวลผลข้อมูลส่วนบุคคล
- ระยะเวลาที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- อาณาเขตทางภูมิศาสตร์ที่ถูกครอบคลุม กล่าวคือ กิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นครอบคลุมไปถึงการดำเนินการที่ต่างประเทศหรือไม่ อย่างไร

(3) บริบทในการประมวลผลข้อมูลส่วนบุคคล คือ ภาพรวม ซึ่งรวมไปถึงปัจจัยภายในและภายนอกที่อาจทำให้เกิดผลกระทบหรือมีผลกระทบต่อความคาดหวังเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมถึงตัวอย่างดังต่อไปนี้

- แหล่งที่มาของข้อมูลส่วนบุคคล
- สภาพความสัมพันธ์ระหว่างบริษัทกับเจ้าของข้อมูลส่วนบุคคล
- เจ้าของข้อมูลส่วนบุคคลห่างไกลจากการควบคุมข้อมูลส่วนบุคคลของตนมากเพียงใด

- เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลได้มากนักน้อยเพียงใด
- มีผู้เยาว์หรือบุคคลที่เปราะบางเป็นเจ้าของข้อมูลส่วนบุคคลรวมอยู่ด้วยหรือไม่
- บริษัทมีประสบการณ์ในการประมวลผลข้อมูลส่วนบุคคลในลักษณะนี้เพียงใด
- มีความก้าวหน้าทางด้านเทคโนโลยีและความมั่นคงปลอดภัยเพียงใด
- มีความกังวลของสาธารณะหรือไม่

(4) วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล คือ เหตุผลที่บริษัทต้องการที่จะประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงตัวอย่างดังต่อไปนี้

- ฐานในการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ผลลัพธ์ของการประมวลผลข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคลที่ตั้งใจเอาไว้
- ผลประโยชน์ต่อบริษัทและสังคมโดยรวมที่คาดหวัง

ขั้นที่ 3 กระบวนการปรึกษาหารือ

บริษัทจะต้องสอบถามและบันทึกความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล (หรือตัวแทนเจ้าของข้อมูลส่วนบุคคล) เว้นเสียแต่ว่าบริษัทมีเหตุผลอันสมควรที่จะไม่บันทึกความคิดเห็นดังกล่าว ซึ่งบริษัทจะต้องให้คำอธิบายที่ชัดเจนในการยกเหตุผลความไม่เหมาะสมที่จะทำการสอบถามความเห็นดังกล่าว เช่น การทำการสอบถามความเห็นดังกล่าวจะทำให้สูญเสียความลับทางการค้า สูญเสียความมั่นคงปลอดภัยของระบบ ไม่ได้สัดส่วน หรือเป็นไปได้ไม่ได้ในทางปฏิบัติ เป็นต้น

หาก DPIA จัดทำขึ้นเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่ได้จากสัญญาที่มีอยู่แล้ว เช่น สัญญาจ้างงาน บริษัทจะต้องทำการสอบถามความเห็นจากเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง กล่าวคือ ลูกจ้าง หรือตัวแทนของเจ้าของข้อมูลส่วนบุคคล อาทิ สหภาพแรงงาน

ส่วน DPIA ที่จัดทำเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่ยังไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด บริษัทอาจทำการสอบถามความเห็นโดยการสอบถามความเห็นของสาธารณะหรือการวิจัยโดยเฉพาะเจาะจง การสอบถามดังกล่าวอาจทำผ่านแบบฟอร์มวิจัยตลาดเฉพาะกลุ่มเป้าหมายหรือการติดต่อกลุ่มเคลื่อนไหวหรือกลุ่มผู้บริโภคที่เกี่ยวข้องเพื่อสอบถาม

ทั้งนี้ หากการตัดสินใจใน DPIA ของบริษัทแตกต่างไปจากความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล บริษัทจะต้องบันทึกเหตุผลที่เห็นต่างจากความเห็นดังกล่าวไว้ด้วย

สำหรับกรณีที่บริษัทจำเป็นต้องได้รับความช่วยเหลือจากผู้ประมวลผลข้อมูลส่วนบุคคล ในกรณีนี้ บริษัทควรที่จะต้องกำหนดหน้าที่ในการให้ความช่วยเหลือบริษัทไว้ในสัญญาด้วย

นอกจากนี้ บริษัทควรที่จะต้องหารือกับผู้มีส่วนได้เสียภายในทุกฝ่าย โดยเฉพาะผู้ที่มีความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยในข้อมูล และแม้จะไม่ได้เป็นการบังคับ แต่ก็จะเป็นแนวทางปฏิบัติที่ดี หากบริษัทได้ทำการหารือหรือปรึกษากับผู้เชี่ยวชาญอิสระอื่น ๆ เช่น ทนายความ นักสังคมวิทยา ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ฯลฯ

ขั้นที่ 4 ประเมินความจำเป็นและความเป็นส่วนตัว

บริษัทควรพิจารณาปัจจัยดังต่อไปนี้เพื่อกำหนดและบันทึกความจำเป็น รวมถึงการได้สัดส่วนในการประมวลผลข้อมูลส่วนบุคคลของบริษัท

- แผนของบริษัทช่วยให้บรรลุวัตถุประสงค์ของบริษัทหรือไม่
- มีวิธีการอื่นที่สมเหตุสมผลที่ทำให้บรรลุผลลัพธ์เดียวกันหรือไม่

แนวทางปฏิบัติของ Working Party 29 (WP29)¹³⁷ ยังแนะนำให้เพิ่มเติมว่าบริษัทจะดำเนินการอย่างไรให้แน่ใจว่าได้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยมีมาตรการที่จำเป็นและได้สัดส่วน ซึ่งรวมถึงรายละเอียดต่อไปนี้

- ฐานในการประมวลผลข้อมูลส่วนบุคคล
- บริษัทจะป้องกันการคลาดเคลื่อนของวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลอย่างไร
- บริษัทจะดำเนินการอย่างไรให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลคุณภาพ
- บริษัทจะดำเนินการอย่างไรให้ใช้ข้อมูลส่วนบุคคลให้น้อยที่สุด
- บริษัทจะให้ความรู้เกี่ยวกับความเป็นส่วนตัวของข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลอย่างไร
- บริษัทจะดำเนินการและสนับสนุนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างไร

¹³⁷ Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, (17/EN, WP 248 rev.01), Adopted on 4 April 2017 as last Revised and Adopted on 4 October 2017

- มาตรการที่ทำให้แน่ใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทจะปฏิบัติตามกฎหมาย
- บริษัทจะให้ความคุ้มครองการโอนข้อมูลส่วนบุคคลไปต่างประเทศอย่างไร

ขั้นที่ 5 ระบุและประเมินความเสี่ยง

ขั้นตอนนี้เป็นขั้นตอนในการพิจารณาความเป็นไปได้ของผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลและผลกระทบต่อความเสียหายจากการประมวลผลข้อมูลส่วนบุคคลนั้นอาจก่อให้เกิด ไม่ว่าจะเป็นทางกายภาพ จิตใจ หรือวัตถุ โดยเฉพาะอย่างยิ่ง พิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนี้จะทำให้เกิดผลกระทบดังต่อไปนี้หรือไม่

- ไม่สามารถมีการใช้สิทธิได้ (ไม่จำกัดเพียงสิทธิในความเป็นส่วนตัว)
- ไม่สามารถเข้าถึงบริการหรือโอกาสได้
- สูญเสียการควบคุมการใช้ข้อมูลส่วนบุคคล
- ถูกกีดกันหรือเหยียด
- ถูกลักทรัพย์หรือฉ้อโกง
- สูญเสียทางการเงิน
- เสียชื่อเสียง
- เสียหายทางกายภาพ
- สูญเสียความลับ
- ถูกระบุตัวตนจากข้อมูลที่ถูกทำให้เป็นข้อมูลนิรนาม
- เกิดความเสียหายเปรียบทางเศรษฐกิจหรือสังคมอย่างมีนัยสำคัญ

บริษัทควรที่จะรวมการประเมินความเสี่ยงต่อความมั่นคงปลอดภัย ซึ่งรวมแหล่งที่มาของความเสี่ยง และผลกระทบที่เป็นไปได้ของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลในแต่ละรูปแบบ (เช่น การเข้าถึงข้อมูลโดยไม่ชอบ การเปลี่ยนแปลงหรือการสูญเสียข้อมูลส่วนบุคคล) ด้วย

ในการประเมินความเสี่ยง บริษัทจำเป็นต้องพิจารณาทั้งความเป็นไปได้ที่จะเกิดผลกระทบและความร้ายแรงของผลกระทบไปพร้อมกัน ทั้งนี้ บริษัทสามารถใช้แผนภาพด้านล่างนี้¹³⁸ในการประเมินความเสี่ยงได้

¹³⁸ ICO, 'How do we do a DPIA?' < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how1> > (accessed 5 June 2020)

ความ ร้าย แรง ของ ผล กระทบ	มีผลกระทบ ร้ายแรง	ความเสี่ยงต่ำ	ความเสี่ยงสูง	ความเสี่ยงสูง
	มีผลกระทบ อยู่บ้าง	ความเสี่ยงต่ำ	ความเสี่ยงปานกลาง	ความเสี่ยงสูง
	มีผลกระทบ เล็กน้อย	ความเสี่ยงต่ำ	ความเสี่ยงต่ำ	ความเสี่ยงต่ำ
		ห่างไกลจาก ความเป็นไปได้ที่จะเกิด ผลกระทบ	มีความเป็นไปได้ พอสมควรที่จะเกิด ผลกระทบขึ้นได้	มีความเป็นไปได้ ที่จะเกิดมากกว่า ที่จะไม่เกิด
		ความเป็นไปได้อาจเกิดผลกระทบ		

นอกจากนี้ บริษัทยังสามารถที่จะทำการประเมินความเสี่ยงต่อตัวบริษัทเองได้ ในแง่ที่เกี่ยวข้องผลกระทบจากการถูกสอบสวนโดยหน่วยงานกำกับดูแล ผลกระทบต่อชื่อเสียงหรือความเชื่อถือจากสาธารณะอีกด้วย

ขั้นที่ 6 ระบุมาตรการลดความเสี่ยง

บริษัทควรที่จะบันทึกแหล่งที่มาของความเสี่ยงทุกความเสี่ยงที่ถูกระบุ และพิจารณาทางเลือกที่จะลดความเสี่ยงดังกล่าว เช่น

- ตัดสินใจที่จะไม่เก็บรวบรวมข้อมูลบางประเภท
- ลดขอบเขตการประมวลผลข้อมูลส่วนบุคคล
- ลดระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล
- เพิ่มมาตรการความปลอดภัยทางเทคโนโลยี

- ฝึกอบรมให้แน่ใจว่าพนักงานหรือลูกจ้างสามารถคาดการณ์และบริหารความเสี่ยงได้
- จัดทำการแบ่งข้อมูลหรือจัดทำให้ข้อมูลเป็นข้อมูลนิรนามเมื่อเป็นไปได้
- จัดทำแนวทางภายในเพื่อหลีกเลี่ยงความเสี่ยง
- ใช้เทคโนโลยีอื่นที่จะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลน้อยกว่าแทน
- ทำสัญญาเปิดเผยข้อมูลส่วนบุคคลระหว่างสองฝ่าย
- เปลี่ยนแปลงนโยบายคุ้มครองข้อมูลส่วนบุคคล
- เสนอทางเลือกให้เจ้าของข้อมูลส่วนบุคคลออกจากกลุ่ม (opt out) เมื่อเหมาะสม
- ดำเนินการจัดทำระบบใหม่เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิได้

ทั้งนี้ อาจมีทางเลือกอื่นนอกเหนือจากที่ได้ยกตัวอย่างมาข้างต้นแล้ว โดยบริษัทสามารถปรึกษากับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทเพื่อหาทางเลือกอื่น ๆ เพื่อลดความเสี่ยงได้เช่นกัน

บริษัทจะต้องบันทึกว่ามาตรการใดช่วยลดหรือกำจัดความเสี่ยง โดยที่บริษัทสามารถพิจารณาถึงต้นทุนและประโยชน์ที่จะได้รับจากมาตรการที่เลือกใช้ เพื่อตัดสินใจเลือกมาตรการที่เหมาะสม

ขั้นที่ 7 การลงชื่อและบันทึกผลสุดท้าย

บริษัทควรที่จะบันทึกรายละเอียดดังต่อไปนี้เพื่อเป็นหลักฐานในการจัดทำ DPIA

- บริษัทมีแผนจะเพิ่มมาตรการใดบ้าง
- ความเสี่ยงใดถูกกำจัด ลด หรือยอมรับแล้วบ้าง
- ระดับความเสี่ยงคงเหลือโดยรวมหลังจากมีการเพิ่มเติมมาตรการ
- บริษัทจะต้องปรึกษารื้อกับหน่วยงานกำกับดูแลหรือไม่

บริษัทไม่จำเป็นต้องกำจัดความเสี่ยงเสมอไป บริษัทสามารถตัดสินใจที่จะยอมรับความเสี่ยงในแต่ละระดับได้ (เล็กน้อย/ ปานกลาง/ สูง) ขึ้นอยู่กับผลประโยชน์ที่ได้รับจากการประมวลผลข้อมูลส่วนบุคคลและความยากลำบากในการบรรเทาผลกระทบ อย่างไรก็ตาม หากความเสี่ยงยังคงสูงอยู่ บริษัทจะต้องหารือกับหน่วยงานกำกับดูแลข้อมูลส่วนบุคคลก่อนเริ่มการประมวลผลข้อมูลส่วนบุคคล

บริษัทจะต้องขอและบันทึกคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในความเห็นเกี่ยวกับการปฏิบัติตามกฎหมายและการเริ่มต้นทำตามแผน ถ้าบริษัทตัดสินใจที่จะไม่ทำตามคำแนะนำดังกล่าว บริษัทก็ควรที่จะบันทึกเหตุผลไว้ด้วย

นอกจากนี้ บริษัทยังควรที่จะต้องบันทึกเหตุผล สำหรับการตัดสินใจที่ตรงข้ามกับความคิดเห็นของเจ้าของข้อมูลส่วนบุคคลและที่ปรึกษาอื่น ๆ ด้วย

ขั้นตอนต่อการจัดทำ DPIA

บริษัทควรที่จะนำเอาผลลัพธ์ที่ได้จากการทำ DPIA กลับเข้าประกอบเป็นส่วนหนึ่งของโครงการหรือแผนธุรกิจของบริษัท โดยที่บริษัทจะต้องกำหนดแผนการดำเนินการและผู้รับผิดชอบในการดำเนินการตามผลลัพธ์ของ DPIA นั้นด้วย

นอกจากนี้ บริษัทยังควรที่จะต้องคอยตรวจสอบ DPIA ของตนให้ทันต่อการเปลี่ยนแปลงอยู่เสมอ โดยการทบทวนและจัดทำ DPIA ขึ้นอีกรอบ สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีการเปลี่ยนแปลง (เช่น การเปลี่ยนแปลงที่มีนัยสำคัญในสภาพ ขอบเขต บริบท หรือวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล)

12.5.6 ตัวอย่างร่างแบบฟอร์มประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Draft Sample of DPIA Template)¹³⁹

ผู้ควบคุมข้อมูลส่วนบุคคลควรเริ่มทำแบบฟอร์มฉบับนี้ เมื่อเริ่มต้นโครงการหรือแผนธุรกิจที่เกี่ยวข้องกับการประมวลผลข้อมูลที่จะต้องจัดทำ DPIA หรือเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการเปลี่ยนแปลงกระบวนการประมวลผลข้อมูลส่วนบุคคลที่ใช้อยู่โดยมีนัยสำคัญ ซึ่งผลสุดท้ายของการจัดทำ DPIA นั้นควรจะต้องถูกรวมเข้าไปในโครงการหรือแผนธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคลด้วย

รายละเอียดเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

ชื่อของผู้ควบคุมข้อมูลส่วนบุคคล	
รายละเอียดการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล/ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	

¹³⁹ ICO, 'DPIA suggested process and template' <https://icosearch.ico.org.uk/s/search.html?query=DPIA&collection=ico-meta&profile=_default> DPIA Template 20180622 v0.4 (accessed 5 June 2020)

ขั้นที่ 1 ระบุเหตุจำเป็นในการจัดทำ DPIA

อธิบายในภาพรวมว่าโครงการหรือแผนธุรกิจนี้มุ่งที่จะบรรลุเป้าหมายอะไร และมีการประมวลผลข้อมูลส่วนบุคคลประเภทใดที่เกี่ยวข้อง (อาจอ้างอิงถึงลิงก์หรือเอกสารอื่น อาทิ ข้อเสนอโครงการ) สรุปเหตุผลในการจัดทำ DPIA

ขั้นที่ 2 อธิบายกระบวนการประมวลผลข้อมูลส่วนบุคคล

อธิบายลักษณะของการประมวลผลข้อมูลส่วนบุคคล:

- วิธีการในการเก็บรวบรวม ใช้ เก็บรักษา และลบข้อมูลส่วนบุคคล
- แหล่งของข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่น
- การประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง

อธิบายขอบเขตของการประมวลผลข้อมูลส่วนบุคคล:

- ข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหวที่เกี่ยวข้อง
- ปริมาณข้อมูลส่วนบุคคลที่จะประมวลผล
- ความถี่ในการประมวลผลข้อมูลส่วนบุคคล
- ระยะเวลาในการเก็บข้อมูลส่วนบุคคล
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่อาจเกี่ยวข้อง
- ขอบเขตพื้นที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

• อธิบายบริบทของการประมวลผลข้อมูลส่วนบุคคล:

● ความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล เช่น ลูกค้า ลูกจ้าง ฯลฯ ● ความสามารถในการควบคุมการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ● ความคาดหวังของเจ้าของข้อมูลส่วนบุคคลว่าเจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้หรือไม่ว่าบริษัทจะใช้ข้อมูลส่วนบุคคล ● กลุ่มเจ้าของข้อมูลส่วนบุคคลมีผู้เยาว์หรือบุคคลที่เปราะบาง ● ข้อกังวล หรือข้อบกพร่องด้านความปลอดภัย ● รูปแบบ หรือลักษณะการประมวลผลข้อมูลส่วนบุคคล ● ความแปลกใหม่ หรือรูปแบบใหม่ที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ● เทคโนโลยีที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ● ข้อกังวลจากสาธารณะที่ท่านควรจะต้องนำมาพิจารณาประกอบการประมวลผลข้อมูลส่วนบุคคล

อธิบายวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล: ● วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ● ผลที่คาดหวังจากการประมวลผลข้อมูลส่วนบุคคลที่บริษัทต้องการให้เกิดกับเจ้าของข้อมูลส่วนบุคคล ● ประโยชน์ของการประมวลผลข้อมูลส่วนบุคคล

ขั้นที่ 3 กระบวนการปรึกษาหารือ

พิจารณาว่าจะต้องหารือกับผู้มีส่วนได้เสียที่เกี่ยวข้องอย่างไร: ● วิธีการ และวันที่ได้สอบถามความเห็นของเจ้าของข้อมูลส่วนบุคคล ● เหตุผลที่เหมาะสมที่ในการไม่ทำการสอบถามความคิดเห็นจากเจ้าของข้อมูลส่วนบุคคล ● บุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ● ผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ● การดำเนินการ และบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ขั้นที่ 4 ประเมินความจำเป็นและความได้สัดส่วน

อธิบายการปฏิบัติตามกฎหมายและมาตรการที่ได้สัดส่วน โดยเฉพาะ:

- ฐานในการประมวลผลข้อมูลส่วนบุคคล
- การบรรลุวัตถุประสงค์จากการประมวลผลข้อมูลส่วนบุคคล
- วิธีการอื่นที่สามารถทำให้ท่านบรรลุผลลัพธ์เดียวกัน
- วิธีการป้องกันการคลาดเคลื่อนของวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล
- วิธีการที่ทำให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นเป็นข้อมูลคุณภาพและปริมาณน้อย
- รายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
- การสนับสนุน และการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- มาตรการที่ทำให้แน่ใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมาย
- วิธีการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการโอนข้อมูลส่วนบุคคลไปต่างประเทศ

ขั้นที่ 5 ระบุและประเมินความเสี่ยง

อธิบายแหล่งของความเสี่ยงและสภาพของผลกระทบที่เป็นไปได้ต่อเจ้าของข้อมูลส่วนบุคคล รวมถึงไปถึงความเสี่ยงเกี่ยวกับการปฏิบัติตามกฎหมายและที่เกี่ยวกับบริษัทตามจำเป็น	ความเป็นไปได้ที่จะเกิดผลกระทบ	ความร้ายแรงของผลกระทบ	ความเสี่ยงในภาพรวม
	ห่างไกลจากความเป็นไปได้ที่จะเกิดผลกระทบ	มีผลกระทบเล็กน้อย	ความเสี่ยงต่ำ
	มีความเป็นไปได้พอสมควรที่จะเกิดผลกระทบขึ้นได้	มีผลกระทบอยู่บ้าง	ความเสี่ยงปานกลาง
	มีความเป็นไปได้ที่จะเกิดผลกระทบมากกว่า	มีผลกระทบร้ายแรง	ความเสี่ยงสูง

	ที่จะไม่เกิด		
--	--------------	--	--

ขั้นที่ 6 ระบุมาตรการลดความเสี่ยง

ระบุมาตรการเพิ่มเติมที่ทำให้ท่านสามารถลดหรือกำจัดความเสี่ยงที่ถูกระบุไว้ในระดับ ปานกลาง หรือ สูง ในขั้นที่ 5				
ความเสี่ยง	ตัวเลือกสำหรับการลดหรือกำจัดความเสี่ยง	ผลกระทบต่อความเสี่ยง	ความเสี่ยงคงเหลือ	มาตรการที่ได้รับอนุมัติ
		กำจัด ความเสี่ยง ความเสี่ยงลดลงในปริมาณที่ยอมรับได้	เล็กน้อย ปานกลาง สูง	ใช่/ไม่ใช่

ขั้นที่ 7 การลงชื่อและบันทึกผลสุดท้าย

รายการ	ชื่อ/ตำแหน่ง/วันที่	หมายเหตุ
มาตรการอนุมัติโดย:		ให้รวมมาตรการเข้าไปเป็นส่วนหนึ่งของโครงการหรือแผนธุรกิจพร้อมกับข้อมูลและความรับผิดชอบในการดำเนินการให้เสร็จสิ้น
ความเสี่ยงคงเหลืออนุมัติโดย:		ถ้ามีการอนุมัติความเสี่ยงคงเหลือระดับสูง ท่านจะต้องหาหรือหน่วยงานกำกับดูแลก่อนเริ่มดำเนินการ
คำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจัดทำแล้ว:		เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎหมายมาตรการในขั้นตอนที่ 6 และเกี่ยวกับว่าสามารถดำเนินการ

		ประมวลผลข้อมูลส่วนบุคคลได้หรือไม่
สรุปคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล		
คำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับการยอมรับหรือปฏิเสธโดย:		ถ้าปฏิเสธ ท่านจะต้องอธิบายเหตุผลของท่านด้วย
ความคิดเห็นของท่าน:		
คำตอบข้อหาหรือได้รับการตรวจสอบโดย:		ถ้าการตัดสินใจของท่านแตกต่างไปจากความเห็นของเจ้าของข้อมูลส่วนบุคคล ท่านจะต้องอธิบายเหตุผลของท่านด้วย
ความคิดเห็นของท่าน:		
DPIA ฉบับนี้ จะได้รับการตรวจสอบโดย:		เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องตรวจสอบการปฏิบัติตามกฎหมายอย่างต่อเนื่องพร้อมกับ DPIA ด้วย

12.6 แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในของบริษัท

เพื่อการจัดการกับข้อมูลส่วนบุคคลภายใน บริษัทอาจจัดให้มีนโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัท เพื่อให้พนักงาน และบุคคลที่เกี่ยวข้องในบริษัทสามารถปฏิบัติตาม และเป็นแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของบริษัท ได้ ทั้งนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในบริษัท

ในการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน บริษัทควรคำนึงถึงการจัดให้มีเนื้อหา และรายละเอียดในหัวข้อต่อไปนี้¹⁴⁰

1. **ชื่อนโยบาย** ในกรณีนี้บริษัทอาจตั้งชื่อนโยบายว่า “นโยบายคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร” ทั้งนี้เพื่อป้องกันไม่ให้เกิดความสับสนเมื่อมีการกล่าวถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลอื่น ๆ ที่ใช้กับบุคลากรภายนอก
2. **วันทีนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในมีผลใช้บังคับ**
3. **บุคคลผู้รับผิดชอบตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน** พร้อมช่องทางการติดต่อบุคคลดังกล่าว เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
4. **ฝ่ายงาน หรือส่วนงานที่นโยบายคุ้มครองข้อมูลส่วนบุคคลภายในใช้บังคับ** กล่าวคือ บุคคลที่ต้องปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน ซึ่งในกรณีนี้บริษัทควรกำหนดให้ชัดเจนโดยกำหนดให้พนักงาน ลูกจ้าง หรือผู้รับจ้างไม่ว่าเป็นการจ้างงานชั่วคราว หรือไม่มีกำหนดระยะเวลาซึ่งมีการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะต้องปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในที่บริษัทจัดทำขึ้น
5. **ประวัติการแก้ไข หรือเปลี่ยนแปลงของนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน**
6. **บุคคลผู้ตรวจสอบ และอนุมัตินโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน พร้อมวันที่ตรวจสอบ และอนุมัติ**
7. **วัตถุประสงค์ของนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน**

¹⁴⁰ Master Writing Policies, Procedures, Processes, and Work Instructions, <https://www.smartsheet.com/company-policies-procedures>, เข้าถึงเมื่อ 1 กันยายน 2563

8. คำจำกัดความของคำที่จะใช้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน โดยอย่างน้อย ควรมีคำจำกัดความตามที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เช่น คำว่า “ข้อมูลส่วนบุคคล” “ผู้ควบคุมข้อมูลส่วนบุคคล” “ผู้ประมวลผลข้อมูลส่วนบุคคล”

9. เนื้อหาของนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน ในส่วนนี้บริษัทสามารถกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลตามความเหมาะสมของบริษัทเอง โดยบริษัทควรเริ่มจากการพิจารณาการดำเนินการ หรือกระบวนการทำงานของบริษัท และพูดคุยถึงประเด็นที่สำคัญเกี่ยวกับการดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจากฝ่ายงานต่าง ๆ เพื่อพิจารณาเนื้อหา และการกำหนดนโยบาย หรือหลักการการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามที่บุคคลที่เกี่ยวข้องเสนอ หรือแสดงความคิดเห็น โดยเนื้อหาของนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในอาจกำหนดให้มีหัวข้อดังต่อไปนี้

9.1 นโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยควรเป็นนโยบายที่สอดคล้องกับกฎหมายลำดับรองเกี่ยวกับมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9.2 นโยบายในการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

9.3 นโยบายในการจัดการกับการร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

9.4 นโยบายในการดำเนินการเมื่อรับทราบถึงการละเมิดข้อมูลส่วนบุคคล

9.5 นโยบายในการจัดการกับข้อมูลส่วนบุคคลทั้งในรูปแบบเอกสาร และอิเล็กทรอนิกส์

9.6 นโยบายในการดำเนินการเมื่อมีข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

9.7 นโยบายในการเปิดเผย และโอนข้อมูลส่วนบุคคล

10. รายชื่อนโยบาย และแนวทางการดำเนินงานอื่น ๆ ของบริษัทที่เกี่ยวข้อง หรือที่มีการอ้างอิงถึงในนโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน

ข้อแนะนำเพิ่มเติม

1. ในการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในเพื่อให้พนักงานปฏิบัติตาม บริษัทควรใช้ภาษาที่อ่านง่าย ไม่ใช้คำศัพท์ทางกฎหมายหากไม่จำเป็น เพื่อให้พนักงาน และบุคคลที่เกี่ยวข้องสามารถเข้าใจถึงเนื้อหาของนโยบาย และสามารถปฏิบัติตามได้อย่างถูกต้อง

2. บริษัทควรกำหนดให้มีการทบทวนนโยบายคุ้มครองข้อมูลส่วนบุคคลเป็นประจำ เช่น กำหนดให้มีการทบทวนนโยบาย 1 ครั้งต่อปี

3. ก่อนที่บริษัทจะนำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในเสนอแก่ผู้มีอำนาจอนุมัตินโยบาย บริษัทอาจส่งร่างนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในให้แก่หน่วยงานที่เกี่ยวข้องเพื่อหารือ หรือขอข้อเสนอแนะเพิ่มเติม

4. เมื่อมีการใช้นโยบายคุ้มครองข้อมูลส่วนบุคคลภายใน บริษัทอาจควรกำหนดให้ฝ่ายทรัพยากรบุคคล (หรือฝ่ายที่เป็นผู้รับผิดชอบในการจัดอบรมของบริษัท) ให้ความรู้ หรืออบรมพนักงาน และบุคคลที่เกี่ยวข้องเพื่อให้บุคคลเหล่านั้นเข้าใจถึงเนื้อหา และวิธีการปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคลอย่างแท้จริง

12.7 สรุปเงื่อนไขการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตามกฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
สิทธิในการเพิก ถอนความยินยอม	✓	✗	✗	✗	✗	✗	✗	สิ่งที่ต้องทำเมื่อมีการใช้สิทธิ 1) ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบของการเพิกถอนความยินยอม 2) จะต้องหยุดประมวลผลข้อมูลส่วนบุคคล ที่อาศัยฐานความยินยอมโดยไม่ล่าช้านับแต่ทราบถึงการใช้สิทธิเพิกถอนความยินยอมนั้น เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างอิงเป็นฐานในการประมวลผลข้อมูลฐานอื่นนอกจากฐานความยินยอมได้	1) มีข้อจำกัดสิทธิในการถอนความยินยอมตามกฎหมาย หรือ 2) มีข้อจำกัดสิทธิในการถอนความยินยอมตามสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล
สิทธิในการเข้าถึง ข้อมูล	✓	✓	✓	✓	✓	✓	✓	1) ในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลเกี่ยวกับตน ซึ่งอยู่ในความรับผิดชอบของบริษัท 2) ขอให้เปิดเผยแหล่งที่มาของข้อมูลส่วนบุคคลของคนที่เจ้าของข้อมูลส่วนบุคคลไม่ได้เป็นผู้ให้ความยินยอมได้ Remark: หากไม่มีข้ออ้างที่จะเป็นเหตุในการปฏิเสธการปฏิบัติตามคำขอดังกล่าวได้ บริษัทจะต้องรีบดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล ไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอดังกล่าว	1) เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล 2) การเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลดังกล่าวจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่นได้ เมื่อ บริษัท ได้ ปฏิเสธ คำขอ ข้าง ต้น แล้ว บริษัทจะต้องบันทึกคำอธิบายและรายละเอียดกรณีการปฏิเสธคำขอในเรื่องเกี่ยวกับการขอสำเนาข้อมูลส่วนบุคคลนั้น
สิทธิแก้ไขข้อมูล	✓	✓	✓	✓	✓	✓	✓	ไม่มีเงื่อนไขในการใช้สิทธิ	ไม่มีเหตุแห่งการปฏิเสธคำขอ

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตาม กฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
สิทธิในการลบ ข้อมูล	✓	✓	✓	✓	✓	✓	✓	เจ้าของข้อมูลส่วนบุคคลในการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (De-identification) ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้ - เมื่อข้อมูลส่วนบุคคลไม่มีความจำเป็นในการเก็บรักษาไว้เพื่อประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อีกต่อไป - เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถอ้างอิงฐานในการประมวลผลข้อมูล ฐานอื่น นอกจากฐานความยินยอมได้ - เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม และผู้ควบคุมข้อมูลส่วนบุคคลไม่มีเหตุในการปฏิเสธคำขอใช้สิทธิดังกล่าวได้ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ก) หรือ(ข)	- การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น - การเก็บรักษาไว้เพื่อวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (1) - การเก็บรักษาไว้เพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ในการดำเนินการภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม ข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอธิปไตยมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (4) - การเก็บรักษาข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษไว้เพื่อวัตถุประสงค์ในเกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 (5) (ก) - การเก็บรักษาข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษไว้เพื่อวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะด้านการสาธารณสุข (มาตรา 26 (5)(ข))

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตาม กฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
								4) เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง 5) เมื่อข้อมูลส่วนบุคคลได้ถูกประมวลผล โดยไม่ชอบด้วยกฎหมาย	6) การใช้เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้อง หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย 7) การปฏิบัติตามกฎหมาย
สิทธิคัดค้าน	✓ สำหรับการ ประมวลผล ข้อมูลส่วน บุคคลเพื่อ การตลาด แบบตรง	✗	✓	✗	✗	✓	✓	1) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ โดยได้รับยกเว้นไม่ต้องขอความยินยอมในกรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม 2) กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง 3) กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับ การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินการกิจ เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล	1. กรณีการประมวลผลอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม 1.1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า 1.2) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น เป็นไปเพื่อ - ก่อตั้งสิทธิเรียกร้องตามกฎหมาย - การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย - การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย 2. กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับ การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตาม กฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
									- เป็นการจำเป็นเพื่อการดำเนินการกิจ เพื่อ ประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วน บุคคล
สิทธิในการระบ การประมวลผล *เงื่อนไขการใช้ สิทธิจะเกี่ยวเนื่อง กับการใช้สิทธิอื่น ได้แก่ 1. สิทธิใน การแก้ไขข้อมูล ส่วนบุคคล 2. สิทธิในการ คัดค้าน 3. สิทธิในการลบ ข้อมูลส่วนบุคคล ส่วน	✓	✓	✓	✓	✓	✓	✓	1) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการ ตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคล ร้องขอให้ ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 36 2) เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลาย เพราะ เป็นข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ หรือเปิดเผย โดยไม่ชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคล ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้แทน 3) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บ รักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมของผู้ ควบคุมข้อมูลส่วนบุคคลแล้ว แต่เจ้าของข้อมูลส่วน บุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อ วัตถุประสงค์ดังต่อไปนี้ - เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตาม กฎหมาย - เพื่อการปฏิบัติตามหรือการใช้สิทธิ เรียกร้องตามกฎหมาย	1) กรณีที่บริษัทพิสูจน์ได้ว่าข้อมูลส่วนบุคคลที่มีอยู่ถูกต้อง สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด 2) กรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิข้างต้น โดยอ้าง ว่าบริษัทไม่มีความจำเป็นในการเก็บรักษาไว้ตาม วัตถุประสงค์ในการเก็บรวบรวมของผู้ควบคุมข้อมูล ส่วนบุคคลแล้ว แต่บริษัทสามารถพิสูจน์ได้ว่า บริษัท ยังมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลอยู่ 3) กรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิข้างต้น โดยยัง ไม่ได้ใช้สิทธิคัดค้านการประมวลผลข้อมูล (บริษัทควร จะต้องมั่นใจว่า บริษัทสามารถพิสูจน์โดยเข้าช้อยกเว้น หรือเหตุปฏิเสธที่จะไม่ปฏิบัติตามสิทธิคัดค้านการ ประมวลผลข้อมูลเสียก่อนที่จะอ้างเหตุปฏิเสธนี้)

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตาม กฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
								- เพื่อการยกขึ้นต่อผู้สิทธิเรียกร้องตามกฎหมาย 4) เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า ในกรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม ผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 32 (1) (ก) 5) เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า ในกรณีการประมวลผลข้อมูลส่วนบุคคลโดยอ้างอิงฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลภายใต้วัตถุประสงค์ดังต่อไปนี้ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 32(1)(ข) - เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย - เพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย - เพื่อการยกขึ้นต่อผู้สิทธิเรียกร้องตามกฎหมาย	

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตาม กฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
								6) เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ว่า การประมวลผลข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ที่เป็นไปเพื่อความจำเป็นในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล	
สิทธิให้โอนย้ายข้อมูล	✓	✓	✗	✗	✗	✗	✗	ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิขอให้โอนย้ายข้อมูลข้างต้น จะต้องเป็นข้อมูลส่วนบุคคลดังต่อไปนี้เท่านั้น 1) เป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอม ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่งพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2) เป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม เพราะเป็นข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมไว้เพื่อความจำเป็นในการประมวลผลข้อมูล ในฐานสัญญาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมาตรา 24 (3)	1) การส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ เช่น กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานรัฐที่ปฏิบัติภารกิจของรัฐ 2) การส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่ตามกฎหมาย 3) การใช้สิทธิข้างต้นนั้น ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น

สรุปเงื่อนไขและสิทธิปฏิเสธการใช้สิทธิ									
	ความ ยินยอม	ฐาน สัญญา	ฐาน ประโยชน์ อันชอบ ธรรม	ฐาน หน้าที่ ตามกฎหมาย	ฐาน ประโยชน์ สำคัญต่อ ชีวิต	ฐาน ภารกิจ ของรัฐ	ฐาน จดหมาย เหตุ/ วิจัย/ สถิติ	เงื่อนไขการใช้สิทธิ	เหตุปฏิเสธการใช้สิทธิ
								3) เป็นข้อมูลส่วนบุคคลอื่นที่กำหนด ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 24 ตามที่คณะกรรมการประกาศกำหนด (ซึ่งปัจจุบัน คณะกรรมการยังไม่ได้ประกาศกำหนด)	
สิทธิร้องเรียน	✓	✓	✓	✓	✓	✓	✓	ขั้นตอนการยื่น การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาเรื่องร้องเรียน จะเป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด	

12.8 การไหลเวียนของข้อมูลส่วนบุคคล (Data Flow) สำหรับบริษัท

12.8.1 การไหลเวียนของข้อมูล (Data Flow) การประกันวินาศภัย (ภาพรวม)

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
การรับ ประกันภัย	- เพื่อทำ สัญญา ประกันภัย - เพื่อติดต่อ สื่อสาร เช่น ขอข้อมูลเพิ่ม ประกอบการ พิจารณา ประกันภัย/ แจ้งผลการรับ ประกันภัย ฯลฯ	<u>ข้อมูลส่วนบุคคล ทั่วไป</u> - ชื่อ-นามสกุล - เลขบัตร ประชาชน/ เลขที่ หนังสือเดินทาง - วัน เดือน ปีเกิด - ที่อยู่ผู้เอา ประกันภัย (ที่อยู่ ตามบัตร ประชาชน/ที่อยู่ ปัจจุบัน - หมายเลข โทรศัพท์	<u>ออฟไลน์</u> - ใบคำขอเอา ประกันภัย - แจ้งผ่านทาง โทรศัพท์ - แจ้งผ่านคน กลาง ประกันภัย/ คู่ ค้าทางธุรกิจ <u>ออนไลน์</u> - อีเมล - เว็บไซต์	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าส่ง ใบคำขอฯ หรือแจ้งความ ประสงค์ขอทำ ประกันภัย ผ่านคนกลาง ประกันภัย หรือ ช่อง ทางการรับ ประกันภัย ต่างๆ	เมื่อลูกค้าส่ง แบบฟอร์มแจ้ง เปลี่ยนแปลง ข้อมูล /ติดต่อ ผ่าน call center เพื่อ ปรับปรุงข้อมูล/ ขอรับบริการ ประกันภัย	10 ปี สูงสุดตาม กฎหมาย ป่ง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่ สามารถระบุตัวตน ได้ (Anonymization)	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่าย ขาย/ฝ่าย บริการ กรมธรรม์ ประกันภัย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ระบบ (ระบุ ชื่อระบบที่เก็บ) - คอมพิวเตอร์ ส่วนบุคคล ของ	- สำนักงาน คปภ. - สมาคมประกัน วินาศภัยไทย - คนกลาง ประกันภัย (ถ้า มี) - บริษัทบริหาร จัดการสินไหม หรือสำรวจภัย (ถ้ามี) - บริษัท ประกันภัยต่อ หรือบริษัท	- ผู้รับ ประกันภัยต่อ ต่างประเทศ (ถ้ามี) - บริษัทแม่ใน ต่างประเทศ (ถ้ามี) - ผู้ให้บริการ เก็บข้อมูล (Cloud) ¹⁴¹

¹⁴¹ กรณีผู้ให้บริการเก็บข้อมูล ไม่รวมการ transit ข้อมูล

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
	- เพื่อจัดส่ง กรมธรรม์ ประกันภัย - เพื่อการแจ้ง การต่ออายุ กรมธรรม์ ประกันภัย - เพื่อจัดการ กรมธรรม์ ประกันภัย/ สลักหลัง (ถ้า มี) - เพื่อจัดทำ ข้อมูลสถิติ ประกันภัย	- อีเมล - อาชีพ และ สถานที่ทำงาน - เพศ - สัญชาติ - ลายมือชื่อผู้ทำ ธุรกรรม (ถ้ามี) - ที่ตั้งทรัพย์สินที่ เอาประกันภัย (ประกันภัย ทรัพย์สิน) - ทรัพย์สินที่เอา ประกันภัย อาทิ สำเนาทะเบียนรถ - ผู้ชำระเบี้ย ประกันภัย - ผู้รับประกันภัย - ผู้รับประกันภัย - ผู้ถือกรมธรรม์ ประกันภัย	- Mobile Application - Line - Facebook						พนักงานที่ดูแล (ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)	ประกันภัยร่วม (ถ้ามี) - สถานพยาบาล	

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		<u>ข้อมูลส่วนบุคคลที่ มีความอ่อนไหว</u> 1) เชื้อชาติ/ สัญชาติ (ประกันภัย อุบัติเหตุ และ สุขภาพ) 2) ข้อมูลสุขภาพ (ประกันภัย อุบัติเหตุ และ สุขภาพ) 3) ข้อมูลส่วน บุคคลเกี่ยวกับ ความพิการ (ประกันภัย อุบัติเหตุ และ สุขภาพ)									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		4) ข้อมูล พันธุกรรม (ประกันภัย อุบัติเหตุ และ สุขภาพ)									
การ จัดการ สินไหม ทดแทน	- เพื่อพิจารณา ค่าสินไหม ทดแทนตาม สัญญา ประกันภัย - เพื่อ ประกอบการ เรียกร้องผู้ทำ ละเมิด เช่น ข้อมูลรับ ประกันภัย พ.ร.บ. ประกันภัย ภาคสมัครใจ ประเภท 1-5	<u>ข้อมูลส่วนบุคคล ทั่วไป</u> ของผู้เรียกร้องค่า สินไหมทดแทน หรือผู้ที่เกี่ยวข้อง ในการพิจารณา จ่ายสินไหม ทดแทน (เช่น ผู้ เอาประกันภัย/ ผู้ ขับซึ้งรถเอา ประกันภัย/ ผู้รับ ประโยชน์ตาม กรมธรรม์ ประกันภัยหรือ ทายาทของผู้เอา	<u>ออฟไลน์</u> - แบบฟอร์ม เรียกร้อง สินไหมทดแทน <u>ออนไลน์</u> - อีเมล - ระบบ e-Claim - ระบบข้อมูล ของ สถานพยาบาล	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าแจ้ง เหตุ/เรียกร้อง ค่าสินไหม ทดแทน	เมื่อลูกค้าส่ง เอกสาร ประกอบการ เรียกร้องค่า สินไหมทดแทน	10 ปี สูงสุดตาม กฎหมาย ป.ง.	<u>เอกสารต้นฉบับ (Hard Copy)</u> - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่ สามารถอ่านได้	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่าย สินไหม - เก็บที่ฝ่าย เรียกร้อง <u>ข้อมูลอิเล็กทรอนิกส์</u> - ระบบ (ระบบ ชื่อระบบที่เก็บ) - คอมพิวเตอร์ ส่วนบุคคล ของ พนักงานที่ดูแล (ถ้ามี) - หน่วยกู้ภัย	- ผู้ให้บริการ บุคคลภายนอก เช่น ผู้ช่วย รถยนต์ ร้าน อะไหล่ โรงพยาบาล ผู้สำรวจภัย - บริษัท ประกันภัยคู่กรณี หรือที่เกี่ยวข้อง - ผู้ให้ความ บริการช่วยเหลือ ฉุกเฉินใน ประเทศ - หน่วยกู้ภัย	- ผู้รับ ประกันภัยต่อ ต่างประเทศ (ถ้ามี) - ผู้ให้ความ บริการ ช่วยเหลือ ฉุกเฉินใน ต่างประเทศ เช่น ผู้สำรวจ ภัยใน ต่างประเทศ

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
	(ประกันภัย ยานยนต์) - เพื่อพิจารณา ตามสัญญา สิทธิการ เรียกร้อง (KFK) (ประกันภัย ยานยนต์) - เพื่อจัดส่ง เอกสาร เรียกร้อง (ถ้า มี)	ประกันภัย/คู่กรณี/ ผู้เกี่ยวข้องอื่นๆ อันได้แก่ข้อมูล ดังต่อไปนี้ - ชื่อ-นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปีเกิด - หมายเลข โทรศัพท์ - อีเมล - อาชีพและ สถานที่ทำงาน - ที่อยู่ปัจจุบัน/ ที่ อยู่ตามบัตร ประชาชน - ลายมือชื่อผู้ เรียกร้องค่าสินไหม ทดแทนหรือผู้ที่ เกี่ยวข้องในการ							- Shared Folder ของ แผนก (ถ้ามี)	- บริษัท กลาง คุ้มครอง ผู้ประสบภัยจาก รถ จำกัด - สำนักงาน คปภ. - สำนักงาน อนุญาตตุลาการ สมาคมประกัน วินาศภัยไทย - หน่วยงานรัฐ เช่น สำนักงาน ตำรวจแห่งชาติ/ สำนักงาน ปปง. เป็นต้น	

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		พิจารณาจ่าย สินไหมทดแทน - เพศ - สัญชาติ - รายละเอียด ความเสียหายซึ่ง อาจมีข้อมูล เกี่ยวข้องหรือ เชื่อมโยงไปถึง ข้อมูลส่วนบุคคล เช่น ทะเบียนรถ ทะเบียนบ้าน โฉนดที่ดิน ฯลฯ - ข้อมูลบัญชี ธนาคารเพื่อจ่ายค่า สินไหมทดแทน - ข้อมูลการชดใช้ ค่าสินไหมทดแทน จากบริษัท ประกันภัยฝ่ายผิด									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		<u>ข้อมูลส่วนบุคคลที่ มีความอ่อนไหว</u> เช่น - ข้อมูลการ เจ็บป่วย/การรักษา (ประกันภัย อุบัติเหตุ และ สุขภาพ) - ข้อมูลประวัติ อาชญากรรม (เช่น บันทึกประจำวัน สำนวนการ สอบสวน หรือ เอกสารทางคดี ฯลฯ) (ประกันภัย อุบัติเหตุ และ สุขภาพ) - ข้อมูลทางนิติ วิทยาศาสตร์ อาทิ									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		ชั้นสูตรพลิกศพ (ประกันภัย อุบัติเหตุ และ สุขภาพ) - ข้อมูลละเมิด (เช่น บันทึก ประจำวันสำนวน การสอบสวน หรือ เอกสารทางคดี เป็นต้น) (ประกันภัยยาน ยนต์)									

12.8.2 การไหลเวียนของข้อมูล (Data Flow) การประกันภัยรถยนต์

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
รับ ประกันภัย	- เพื่อทำ สัญญา ประกันภัย - เพื่อติดต่อ สื่อสาร เช่น ขอข้อมูลเพิ่ม ประกอบการ พิจารณา ประกันภัย/ แจ้งผลการรับ ประกันภัย เป็นต้น - เพื่อจัดส่ง กรมธรรม์ ประกันภัย	<u>ข้อมูลส่วนบุคคล</u> - ชื่อ-นามสกุล - เลขบัตร ประชาชน - เลขที่ ใบอนุญาตขับขี่ - วัน เดือน ปี เกิด - หมายเลข โทรศัพท์ - อีเมล - เพศ - ทรัพย์สินที่ เอาประกันภัย เช่น สำเนา	<u>ออฟไลน์</u> - ใบคำขอเอา ประกันภัย - แจ้งผ่านทาง โทรศัพท์ - แจ้งผ่านคน กลาง ประกันภัย/คู่ ค้าทางธุรกิจ <u>ออนไลน์</u> - อีเมลล์ - เว็บไซต์ - Mobile Application	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าส่ง ใบคำขอฯ หรือแจ้ง ความ ประสงค์ขอ ทำประกันภัย ผ่านคนกลาง ประกันภัย	เมื่อลูกค้า ติดต่อบริษัท หรือแจ้งความ ประสงค์ผ่าน คนกลาง ประกันภัย เพื่อ เปลี่ยนแปลง ข้อมูล	10 ปี สูงสุด ตาม กฎหมาย ป่ง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ส่งเก็บศูนย์เก็บ เอกสาร - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่ สามารถระบุตัวตนได้ (Anonymization)	<u>เอกสารต้นฉบับ</u> - ส่งเก็บศูนย์ เก็บเอกสาร - เก็บที่ฝ่าย ขาย/ฝ่ายบริการ กรมธรรม์ ประกันภัย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ระบบ DMS (Document Management System)	- สำนักงาน คปภ. - สมาคมประกัน วินาศภัยไทย - คนกลาง ประกันภัย - บริษัท ประกันภัยต่อ หรือบริษัท ประกันภัยร่วม	- บริษัทแม่ใน ต่างประเทศ - ผู้รับประกันภัยต่อ ต่างประเทศ - บริษัทแม่ใน ต่างประเทศ - ผู้ให้บริการเก็บ ข้อมูล (Cloud) ¹⁴²

¹⁴² กรณีผู้ให้บริการเก็บข้อมูล ไม่รวมการ transit ข้อมูล

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
	- เพื่อการแจ้ง การต่ออายุ กรมธรรม์ ประกันภัย	ทะเบียนรถ เป็นต้น <u>ข้อมูลส่วนบุคคลที่มีความ อ่อนไหว</u> - ไม่มี	- API (Application Programming Interface) - Social Media, i.e. Line						- คอมพิวเตอร์ ส่วนบุคคล ของ พนักงานที่ดูแล - Shared Folder ของ แผนก		
การ เรียกร้องค่า สินไหม ทดแทน คู่กรณีมี ประกันภัย	- เพื่อ ประกอบการ เรียกร้องผู้ทำ ละเมิด เช่น ข้อมูลรับ ประกันภัย พ.ร.บ. ประกันภัย ภาคสมัครใจ ประเภท 1-5 เป็นต้น - เพื่อ พิจารณาตาม	<u>ข้อมูลส่วนบุคคลทั่วไป</u> -ข้อมูลเคลม จากประกันภัย ฝ่ายผิด จำนวนเงิน ความรับผิด ตามกรมธรรม์ <u>ข้อมูลส่วนบุคคลที่มีความ อ่อนไหว</u> เช่น	<u>ออฟไลน์</u> - ใบรับรอง ความเสียหาย จากประกันภัย คู่กรณี - บันทึกยอมรับ ผิดจากคู่กรณี - บันทึก ประจำวัน <u>ออนไลน์</u> - อีเมล	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	วันที่เกิด อุบัติเหตุและ มีบุคคลที่ต้อง รับผิดชอบ กฎหมาย	เมื่อได้รับการ ชดใช้ค่า สินไหม ทดแทนจาก บริษัท ประกันภัย	10 ปี สูงสุดตาม กฎหมาย ป่ง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่าย เรียกร้อง <u>ข้อมูลอิเล็กทรอนิกส์</u> - ระบบ (ระบุ ชื่อระบบที่เก็บ) - Shared Folder ของ แผนก (ถ้ามี)	- บริษัท ประกันภัยคู่กรณี หรือที่เกี่ยวข้อง เช่น ชนกันหลาย ราย - สำนักงาน อนุญาตตุลาการ สมาคมประกัน วินาศภัยไทย	ไม่มี

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
	สัญญาสละ สิทธิการ เรียกร้อง (KFK) - เพื่อจัดส่ง เอกสาร เรียกร้อง - เพื่อ พิจารณา เรียกร้องค่า สินไหม ทดแทนตาม สัญญา ประกันภัย	- ข้อมูลละเมิด (เช่น บันทึก ประจำวัน สำนวนการ สอบสวน หรือ เอกสารทางคดี เป็นต้น)	- ระบบ e- Claim								
การ เรียกร้องค่า สินไหม ทดแทน คู่กรณีไม่มี ประกันภัย	-เพื่อพิจารณา เรียกร้องค่า สินไหม ทดแทนตาม สัญญา ประกันภัย	<u>ข้อมูลส่วนบุคคลทั่วไป</u> ของผู้ทำ ละเมิด(คู่กรณี) หรือผู้ที่ เกี่ยวข้องใน	<u>ออฟไลน์</u> -ใบรับรองความ เสียหายจาก ประกันภัยคู่กรณี -บันทึกยอมรับ ผิดจากคู่กรณี	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	วันที่เกิด อุบัติเหตุ และมีบุคคล ที่ต้องรับผิดชอบ ตามกฎหมาย	เมื่อได้รับการ ชดใช้ค่า สินไหม ทดแทนจาก บุคคลผู้ทำ ละเมิด	10 ปี สูงสุดตาม กฎหมาย ป่ง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่าย เรียกร้อง <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u>	- ผู้ให้บริการเรียก เก็บหนี้ที่ได้รับ อนุญาตตาม พ.ร.บ. ทวงถาม หนี้ พ.ศ 2558 - ศาล	ไม่มี

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		การขอใช้ (เช่น นายจ้าง ข้อมูล ดังต่อไปนี้ - ชื่อ-นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปี เกิด - หมายเลข โทรศัพท์ - อีเมล - รายละเอียด ความเสียหาย ซึ่งอาจมีข้อมูล เกี่ยวข้องหรือ เชื่อมโยงไปถึง ข้อมูลส่วน บุคคล เช่น ทะเบียนรถ เป็นต้น	-บันทึก ประจำวัน <u>ออนไลน์</u> - อีเมล - เว็บไซต์ - Mobile Application - Line						- ระบบ (ระบุ ชื่อระบบที่เก็บ) - คอมพิวเตอร์ ส่วนบุคคล ของ พนักงานที่ดูแล (ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)		

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของ ข้อมูลส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		ข้อมูลส่วนบุคคลที่มีความ อ่อนไหว - ข้อมูลละเมิด (เช่น บันทึก ประจำวัน สำนวนการ สอบสวน หรือ เอกสารทางคดี เป็นต้น)									

12.8.3 การไหลเวียนของข้อมูล (Data Flow) การประกันภัยขนส่งทางทะเลและโลจิสติกส์

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
การรับประกันภัย	- เพื่อทำสัญญาประกันภัย - เพื่อติดต่อสื่อสาร เช่น ขอข้อมูลเพิ่มเติมประกอบการพิจารณารับประกันภัย/ แจ้งผลการรับประกันภัย เป็นต้น - เพื่อจัดส่งกรมธรรม์ประกันภัย	<u>ข้อมูลส่วนบุคคลทั่วไป</u> - ชื่อ-นามสกุล - เลขบัตรประชาชน - วัน เดือน ปี เกิด - หมายเลขโทรศัพท์ - อีเมล - เพศ - สัญชาติ	<u>ออฟไลน์</u> - ใบคำขอเอาประกันภัย - แจ้งผ่านทางโทรศัพท์ - แจ้งผ่านคนกลาง - ประกันภัย/คู่ค้าทางธุรกิจ <u>ออนไลน์</u> - อีเมล - เว็บไซต์	- พ.ร.บ. ข้อมูลส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าส่งใบคำขอฯ หรือแจ้งความประสงค์ขอทำประกันภัยผ่านคนกลางประกันภัย	เมื่อลูกค้าส่งแบบฟอร์มแจ้งเปลี่ยนแปลงข้อมูล /ติดต่อผ่าน call center เพื่อปรับปรุงข้อมูล/ขอรับบริการประกันภัย	10 ปี สูงสุดตามกฎหมาย ปก.ข้อมูล	<u>เอกสารต้นฉบับ (Hard Copy)</u> - ส่งเก็บศูนย์เก็บข้อมูล - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่สามารถระบุตัวตนได้ (Anonymization)	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่ายขาย/ฝ่ายบริการ - กรมธรรม์ประกันภัย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ระบบ (ระบุชื่อระบบที่เก็บ)	- สำนักงาน คปภ. - สมาคมประกันวินาศภัยไทย - ตัวกลางประกันภัย (ถ้ามี) - บริษัท - บริษัทประกันภัยต่อหรือบริษัทประกันภัยร่วม (ถ้ามี)	- ผู้รับประกันภัยต่อต่างประเทศ (ถ้ามี) - บริษัทแม่ในต่างประเทศ (ถ้ามี) - ผู้ให้บริการเก็บข้อมูล (Cloud) ¹⁴³

¹⁴³ กรณีผู้ให้บริการเก็บข้อมูล ไม่รวมการ transit ข้อมูล

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
	- เพื่อการแจ้ง ต่ออายุ กรมธรรม์ ประกันภัย ประกันภัย	- ข้อมูล ยานพาหนะ ที่เอา ประกันภัย เช่น สำเนา ทะเบียนรถ เป็นต้น <u>ข้อมูลส่วน บุคคลที่มี ความ อ่อนไหว</u> - ไม่มี	- Mobile Application - Line - Facebook						- คอมพิวเตอร์ ส่วนบุคคล ของพนักงาน ที่ดูแล (ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)		

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
การจัดการ สินไหม ทดแทน	เพื่อพิจารณาค่า สินไหมทดแทน ตามสัญญา ประกันภัย	<u>ข้อมูลส่วนบุคคลทั่วไป</u> ของผู้ เรียกร้องค่า สินไหม ทดแทนหรือ ผู้ที่เกี่ยวข้อง ในการ พิจารณา จ่ายสินไหม ทดแทน (เช่นผู้เอา ประกันภัย / คู่กรณี/ ผู้ที่ มีส่วนได้เสีย หรือผู้ที่มี สิทธิ์ในการ เรียกร้อง	<u>ออฟไลน์</u> - แบบฟอร์ม เรียกร้อง สินไหมทดแทน <u>ออนไลน์</u> - อีเมล - ระบบ e-Claim	- พ.ร.บ. ข้อมูลส่วน บุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้า แจ้งเหตุ/ เรียกร้องค่า สินไหม ทดแทน	เมื่อลูกค้าส่ง เอกสาร ประกอบการ เรียกร้องค่า สินไหม ทดแทน	10 ปี สูงสุดตาม กฎหมาย ปบง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่ สามารถอ่านได้	<u>เอกสาร</u> <u>ต้นฉบับ</u> - เก็บที่ฝ่าย สินไหม <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ระบบ (ระบุ ชื่อระบบที่เก็บ) - คอมพิวเตอร์ ส่วนบุคคล ของพนักงาน ที่ดูแล (ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)	- ผู้ให้บริการ บุคคลภายนอก เช่น ผู้สำรวจ ภัย - ผู้ให้ความ บริการช่วยเหลือ ฉุกเฉินใน ประเทศ - หน่วยกู้ภัย - สำนักงาน คปภ. - หน่วยงานรัฐ เช่น สำนักงาน ตำรวจแห่งชาติ /สำนักงาน ปบง. เป็นต้น	- ผู้รับ ประกันภัยต่อ ต่างประเทศ (ถ้ามี) - ผู้ให้บริการ บุคคลภายนอก ในต่างประเทศ เช่น ผู้สำรวจภัย ในต่างประเทศ - ผู้ให้ความ บริการ ช่วยเหลือ ฉุกเฉินใน ต่างประเทศ

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		ค่าเสียหาย อันได้แก่ ข้อมูล ดังต่อไปนี้ - ชื่อ นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปีเกิด - หมายเลข โทรศัพท์ - อีเมล - เพศ - สัญชาติ - รายละเอียด ความเสียหาย ซึ่งอาจมี									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		ข้อมูล เกี่ยวข้องหรือ เชื่อมโยงไปถึง ข้อมูลส่วน บุคคล เช่น ทะเบียนรถ เป็นต้น - ข้อมูล บัญชี ธนาคารเพื่อ จ่ายค่า สินไหม ทดแทน <u>ข้อมูลส่วน</u> <u>บุคคลที่มี</u> <u>ความ</u> <u>อ่อนไหว</u>									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภท ของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐาน กฎหมายที่ ไม่ต้องขอ ความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอก บริษัท (ในประเทศ)	ภายนอก บริษัท (ต่างประเทศ)
		- ไม่มี									

12.8.4 การไหลเวียนของข้อมูล (Data Flow) การประกันภัยทรัพย์สิน

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเทศ)
การรับ ประกันภัย	- เพื่อทำสัญญาประกันภัย - เพื่อติดต่อสื่อสาร เช่น ขอข้อมูลเพิ่ม - ประกอบการพิจารณา - รับประกันภัย/แจ้งผลการรับประกันภัย - เป็นต้น - เพื่อจัดส่งกรมธรรม์ - รับประกันภัย	<u>ข้อมูลส่วนบุคคลทั่วไป</u> - ชื่อ-นามสกุล - เลขบัตรประชาชน - ที่อยู่ผู้เอาประกันภัย - สถานที่ตั้งทรัพย์สินที่เอาประกันภัย - วัน เดือน ปีเกิด - หมายเลขโทรศัพท์ - อีเมล - เพศ - สัญชาติ	<u>ออฟไลน์</u> - ใบคำขอเอาประกันภัย - แจ้งผ่านทางโทรศัพท์ - แจ้งผ่านคนกลาง - ประกันภัย/คู่ค้าทางธุรกิจ <u>ออนไลน์</u> - อีเมล - เว็บไซต์ - Mobile Application	- พ.ร.บ. ข้อมูลส่วนบุคคลฯ - มาตรา 24 (3) - มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าส่งใบคำขอฯ หรือแจ้งความประสงค์ขอทำประกันภัยผ่านคนกลาง	เมื่อลูกค้าส่งแบบฟอร์มแจ้งเปลี่ยนแปลงข้อมูล /ติดต่อผ่าน call center เพื่อปรับปรุงข้อมูล/ขอรับบริการประกันภัย	10 ปี สูงสุดตามกฎหมาย ปพ.ก.	<u>เอกสารต้นฉบับ (Hard Copy)</u> - ส่งเก็บศูนย์เก็บข้อมูล - ทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่สามารถระบุตัวตนได้ (Anonymization)	<u>เอกสารต้นฉบับ</u> - เก็บที่ฝ่ายขาย/ฝ่ายบริการ - กรมธรรม์ - ประกันภัย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ระบบ (ระบุชื่อระบบที่เก็บ) - คอมพิวเตอร์ส่วนบุคคล	- สำนักงาน คปภ. - สมาคมประกันวินาศภัยไทย - คนกลาง - ประกันภัย (ถ้ามี) - บริษัท - ประกันภัยต่อหรือบริษัท - ประกันภัยร่วม (ถ้ามี)	- บริษัทประกันภัยต่อต่างประเทศ (ถ้ามี) - นายหน้าประกันภัยต่อต่างประเทศ (ถ้ามี) - ผู้ให้บริการเก็บข้อมูล (Cloud)¹⁴⁴

¹⁴⁴ กรณีผู้ให้บริการเก็บข้อมูล ไม่รวมการ transit ข้อมูล

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเทศ)
	- เพื่อการแจ้ง ต่ออายุ กรมธรรม์ ประกันภัย	- ทรัพย์สินที่เอา ประกันภัย เช่น สำเนาทะเบียนบ้าน โฉนดที่ดิน เป็นต้น <u>ข้อมูลส่วนบุคคลที่ มีความอ่อนไหว</u> - ไม่มี	- Line - Facebook						ของพนักงาน ที่ดูแล(ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)	- ผู้ประเมิน ราคา - สำนักงาน กฎหมาย - ผู้ประเมิน วินาศภัย - นายหน้า ประกันภัย ต่อ	
การจัดการ สินไหม ทดแทน	เพื่อพิจารณาค่า สินไหมทดแทน ตามสัญญา ประกันภัย	<u>ข้อมูลส่วนบุคคล</u> <u>ทั่วไป</u> ของผู้เรียกร้องค่า สินไหมทดแทนหรือ ผู้ที่เกี่ยวข้องในการ พิจารณาจ่ายสินไหม ทดแทน (เช่นผู้เอา ประกันภัย /ผู้รับ ประโยชน์ตาม	<u>ออฟไลน์</u> - แบบฟอร์ม เรียกร้อง สินไหมทดแทน <u>ออนไลน์</u> - อีเมล - ระบบ e- Claim	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้าแจ้ง เหตุ/เรียกร้อง ค่าสินไหม ทดแทน	เมื่อลูกค้าส่ง เอกสาร ประกอบการ เรียกร้องค่า สินไหมทดแทน	10 ปี สูงสุดตาม กฎหมาย บปง.	<u>เอกสารต้นฉบับ</u> (Hard Copy) - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ลบจากระบบ	<u>เอกสาร</u> <u>ต้นฉบับ</u> - เก็บที่ฝ่าย สินไหม ทดแทน <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u>	- ผู้ ให้บริการ บุคคลภาย นอก เช่น ผู้ ประเมิน วินาศภัย ผู้รับเหมาก่อ สร้าง	- ผู้รับ ประกันภัยต่อ ต่างประเทศ (ถ้ามี) - ผู้ให้ความ บริการ ช่วยเหลือ ฉุกเฉินใน ต่างประเทศ

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเทศ)
		กรรมธรรม์หรือ ทายาทของผู้เอา ประกันภัย/คู่กรณี/ ผู้เกี่ยวข้องอื่นๆ อัน ได้แก่ข้อมูล ดังต่อไปนี้ - ชื่อ-นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปีเกิด - หมายเลข โทรศัพท์ - อีเมล - เพศ - สัญชาติ - รายละเอียดความ เสียหายซึ่งอาจมี ข้อมูลเกี่ยวข้องหรือ เชื่อมโยงไปถึง	- ระบบข้อมูล ของ สถานพยาบาล					- ทำให้ข้อมูลไม่ สามารถอ่านได้	- ระบบ (ระบุ ชื่อระบบที่ เก็บ) - คอมพิวเตอร์ ส่วนบุคคล ของพนักงาน ที่ดูแล(ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)	- ผู้ให้ความ บริการ ช่วยเหลือ ฉุกเฉินใน ประเทศ - หน่วยกู้ภัย - สำนักงาน คปภ. - สำนักงาน กฎหมาย - ธนาคาร (ผู้รับ ประโยชน์) - หน่วยงาน รัฐ เช่น สำนักงาน ตำรวจ แห่งชาติ /	

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเทศ)
		ข้อมูลส่วนบุคคล เช่น ทะเบียนบ้าน โฉนดที่ดิน เป็นต้น - ข้อมูลบัญชี ธนาคารเพื่อจ่ายค่า สินไหมทดแทน <u>ข้อมูลส่วนบุคคลที่ มีความอ่อนไหว -</u> ไม่มี								สำนักงาน ปง. เป็น ต้น	

12.8.5 การไหลเวียนของข้อมูล (Data Flow) การประกันภัยเบ็ดเตล็ด

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเท ศ)
การรับ ประกันภัย	<u>ทำสัญญา</u> <u>ประกันภัย</u> - ติดต่อสื่อสาร - ขอข้อมูล เพื่อ ประกอบการ พิจารณา ประกันภัย / แก้ไข / แจ้ง ยกเลิก - แจ้งผลการรับ ประกันภัย - เพื่อจัดการ กรมธรรม์ ประกันภัย/ สลั๊กหลัง - เพื่อแจ้งต่อ อายุ	<u>บุคคลทั่วไป</u> - ชื่อ-นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปีเกิด - หมายเลข โทรศัพท์ - อีเมล - เพศ - ทรัพย์สินที่เอา ประกันภัย <u>ข้อมูลส่วนบุคคลที่มี</u> <u>ความอ่อนไหว</u> - ไม่มี	<u>ใบคำร้อง (ถ้า</u> <u>มี)</u> - แจ้งผ่าน โทรศัพท์ - แจ้งผ่านคน กลาง ประกันภัย/คู่ ค้า <u>ออนไลน์</u> - อีเมล - Website - Mobile App - Line - FB	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ) -	ส่งใบคำขอ หรือแจ้งความ ประสงค์ ขอทำ ประกันภัยผ่าน คนกลาง ประกันภัย	แจ้ง เปลี่ยนแปลง ข้อมูลติดต่อ Call Center	10 ปี สูงสุดตาม กฎหมาย ปบง.	<u>Hard Copy</u> - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ลบออกจากระบบ - ทำให้ข้อมูลไม่ สามารถระบุตัวตน ได้	<u>ต้นฉบับ</u> - เก็บที่ฝ่ายขาย /ฝ่ายบริการ กรมธรรม์ ประกันภัย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ระบบ X		

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเท ศ)
การ จัดการ สินไหม	เพื่อพิจารณา ค่าสินไหม ทดแทนตาม สัญญา ประกันภัย	<u>ข้อมูลส่วนบุคคล ทั่วไป</u> - ผู้เอาประกันภัย - ผู้รับผลประโยชน์ ตามกรมธรรม์ ประกันภัย / ทายาท ของผู้เอาประกันภัย - ชื่อ-นามสกุล - เลขบัตร ประชาชน - วัน เดือน ปีเกิด - หมายเลข โทรศัพท์ - อีเมล - เพศ - ข้อมูลบัญชี ธนาคารเพื่อจ่าย สินไหมทดแทน	<u>ออฟไลน์</u> - แบบฟอร์ม เรียกร้อง สินไหม ทดแทน / เอกสารแจ้ง ความเสียหาย <u>ออนไลน์</u> - อีเมล	- พ.ร.บ. ข้อมูล ส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อผู้เอา ประกันภัยแจ้ง เหตุ / เรียกร้อง สินไหมทดแทน	เมื่อผู้เอา ประกันภัยส่ง เอกสาร ประกอบการ เรียกร้อง สินไหม ทดแทน	10 ปี สูงสุดตาม กฎหมาย ป่ง.	<u>Hard Copy</u> - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ลบออกจากระบบ - ทำให้ข้อมูลไม่ สามารถระบุตัวตน ได้	<u>ต้นฉบับ</u> - เก็บที่ฝ่าย สินไหม <u>ข้อมูล</u> <u>อิเล็กทรอนิกส์</u> - ระบบ X		

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการ เก็บข้อมูล	ฐานกฎหมายที่ ไม่ต้องขอความ ยินยอม	ระยะเวลา เริ่มต้น	การปรับปรุง แก้ไข	ระยะเวลา การเก็บข้อมูล	การจัดการหลัง สิ้นสุดระยะจัดเก็บ	ภายใน หน่วยงาน	ภายนอก หน่วยงาน (ใน ประเทศ)	ภายนอก หน่วยงาน (ต่างประเท ศ)
		ข้อมูลส่วนบุคคลที่มี ความอ่อนไหว - ไม่มี									

12.8.6 การไหลเวียนของข้อมูล (Data Flow) การประกันภัยอุบัติเหตุและสุขภาพ

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูลส่วนบุคคล	ช่องทางการเก็บข้อมูล	ฐานกฎหมายที่ไม่ต้องขอความยินยอม	ระยะเวลาเริ่มต้น	การปรับปรุงแก้ไข	ระยะเวลากา รเก็บข้อมูล	การจัดการหลังสิ้นสุดระยะจัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
การรับประกันภัย	- เพื่อพิจารณารับประกันภัยและทำสัญญาประกันภัย - เพื่อดัดต่อสื่อสาร เช่น ขอข้อมูลเพิ่มเติมประกอบการพิจารณารับประกันภัย/แจ้งผลการรับประกันภัย จัดส่งกรมธรรม์ประกันภัยและการแจ้งการต่อยุทธกรรม	<u>ข้อมูลส่วนบุคคลทั่วไป (ตาม KYC) - ข้อมูลผู้เอาประกันภัยประกอบด้วย</u> 1) ชื่อ-นามสกุล 2) เลขบัตรประชาชน/เลขที่หนังสือเดินทาง 3) วัน เดือน ปีเกิด 4) หมายเลขโทรศัพท์ 5) อีเมล 6) อาชีพ และสถานที่ทำงาน	<u>ออฟไลน์</u> 1) ใบคำขอลาประกันภัย 2) แจ้งผ่านทางโทรศัพท์ 3) แจ้งผ่านคนกลาง ประกันภัย/ คู่ค้าทางธุรกิจ <u>ออนไลน์</u> 1) อีเมล 2) เว็บไซต์ 3) Mobile Application 4) Line	- พ.ร.บ. ข้อมูลส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ) <u>ออนไลน์</u> ข้อมูลส่วนบุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ) 1) อีเมล 2) เว็บไซต์ 3) Mobile Application 4) Line	เมื่อลูกค้าส่งใบคำขอหรือแจ้งเปลี่ยนแปลงข้อมูลติดต่อผ่าน call center ตัวแทน/นายหน้า/คู่ค้าทางธุรกิจเพื่อปรับปรุงข้อมูล/ขอรับบริการประกันภัย	เมื่อลูกค้าส่งแบบฟอร์มแจ้งเปลี่ยนแปลงข้อมูลติดต่อผ่าน center นายหน้า/คู่ค้าทางธุรกิจเพื่อปรับปรุงข้อมูล/ขอรับบริการประกันภัย	10 ปี สูงสุดตามกฎหมาย ปง.	<u>เอกสารต้นฉบับ (Hard Copy)</u> - ส่งเก็บศูนย์เก็บข้อมูลทำลาย <u>ข้อมูลอิเล็กทรอนิกส์</u> - ลบจากระบบ - ทำให้ข้อมูลไม่สามารถระบุตัวตนได้ (Anonymization)	<u>เอกสารต้นฉบับเก็บที่ฝ่ายขาย/ฝ่ายบริการ กรมธรรม์ ประกันภัย</u> <u>ข้อมูล อิเล็กทรอนิกส์</u> - ระบบ (ระบบชื่อระบบที่เก็บ) - คอมพิวเตอร์ ส่วน บุ คคล ของพนักงาน ที่ดูแล (ถ้ามี)	1) สำนักงาน คปภ. 2) สมาคมประกันวินาศภัยไทย 3) คนกลาง ประกันภัย (ถ้า มี) 4) บริษัท ประกันภัยต่อ หรือบริษัท ประกันภัยร่วม (ถ้ามี) 5) บริษัทรักษา การสินไหม หรือสำรวจภัย (ถ้ามี)	1) ผู้รับประกันภัยต่อต่างประเทศ (ถ้ามี) 2) บริษัทแม่ใน ต่างประเทศ (ถ้ามี) 3) ผู้ให้บริการเก็บข้อมูล (Cloud) ¹⁴⁵

¹⁴⁵ กรณีผู้ให้บริการเก็บข้อมูล ไม่รวมการ transit ข้อมูล

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการเก็บ ข้อมูล	ฐานกฎหมาย ที่ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะ จัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
	ประกันภัย เป็น ต้น - เพื่อจัดทำ ข้อมูลสถิติ ประกันภัย	7) ที่อยู่ปัจจุบัน/ ที่ อยู่ตามบัตร ประชาชน 8) ลายมือชื่อผู้ทำ ธุรกรรม 9) เพศ - ผู้ชำระเบี้ย ประกันภัย - ผู้รับประกันภัย - ผู้รับประกันภัย - ผู้ถือกรมธรรม์ ประกันภัย <u>ข้อมูลส่วนบุคคลที่ มีความอ่อนไหว (ตามใบคำขอเอา ประกันภัย)</u> 1) เชื้อชาติ/ สัญชาติ 2) ข้อมูลสุขภาพ	5) Facebook						- Shared folder ของ แผนก (ถ้ามี)	6) สถานพยาบาล	

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการเก็บ ข้อมูล	ฐานกฎหมาย ที่ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะ จัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		3) ข้อมูลส่วนบุคคลเกี่ยวกับ ความพิการข้อมูล พันธุกรรม									
จัดการ สินไหม ทดแทน	เพื่อพิจารณา ค่าสินไหม ทดแทนตาม สัญญา ประกันภัย	ข้อมูลส่วนบุคคล ทั่วไป ผู้เรียกร้องค่า สินไหมทดแทน หรือผู้ที่เกี่ยวข้องใน การพิจารณาจ่าย สินไหมทดแทน เช่น ผู้เอา ประกันภัย/ผู้ถือ กรรมสิทธิ์ ประกันภัย/ผู้รับ ประโยชน์ตาม	ออฟไลน์ แบบฟอร์ม เรียกร้องสินไหม ทดแทน ออนไลน์ 1) อีเมล 2) ระบบ e - Claim 3) ระบบข้อมูลของ สถานพยาบาล	- พ.ร.บ. ข้อมูลส่วน บุคคลฯ มาตรา 24 (3) มาตรา 26 (4) หรือ 26 (5) (จ)	เมื่อลูกค้า แจ้งเหตุ/ เรียกร้องค่า สินไหม ทดแทน	เมื่อลูกค้าส่ง เอกสาร ประกอบการ เรียกร้องค่า สินไหม ทดแทน	10 ปี สูงสุดตาม กฎหมาย ป่ง.	เอกสารต้นฉบับ (Hard Copy) - ส่งเก็บศูนย์เก็บ ข้อมูล - ทำลาย ข้อมูล อิเล็กทรอนิกส์ - ลบจากระบบ - ทำให้ข้อมูลไม่ สามารถอ่านได้	เอกสาร ต้นฉบับ เก็บที่ฝ่าย สินไหม ข้อมูล อิเล็กทรอนิกส์ - ระบบ (ระบุ ชื่อระบบที่ เก็บ) - คอมพิวเตอร์ ส่วนบุคคล	1) ผู้ให้บริการ บุคคลภายนอก เช่น สถานพยาบาล /ผู้ให้ความ บริการช่วยเหลือ ฉุกเฉินในประเทศ 3) สำนักงาน คปภ. 4) หน่วยงานรัฐ เช่น สำนักงาน ตำรวจแห่งชาติ /	1) ผู้รับประกันภัย ต่อต่างประเทศ (ถ้า มี) 2) สถานพยาบาล ต่างประเทศ 3) ผู้ให้ความ บริการช่วยเหลือ ฉุกเฉินใน ต่างประเทศ

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการเก็บ ข้อมูล	ฐานกฎหมาย ที่ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะ จัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		กรรมธรรม์ ประกันภัยหรือ ทายาทของผู้เอา ประกันภัย/คู่กรณี ผู้เกี่ยวข้องอื่น ๆ อันประกอบด้วย ข้อมูลดังต่อไปนี้ 1) ชื่อ นามสกุล 2) เลขบัตร ประชาชน/เลขที่ หนังสือเดินทาง 3) วัน เดือน ปีเกิด 4) หมายเลข โทรศัพท์ 5) อีเมล 6) อาชีพ และ สถานที่ทำงาน 7) ที่อยู่ปัจจุบัน/ที่ อยู่ตามบัตร ประชาชน							ของพนักงาน ที่ดูแล (ถ้ามี) - Shared Folder ของ แผนก (ถ้ามี)	สำนักงาน ปปง. สำนักงาน กฎหมาย /ศาล เป็นต้น	

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการเก็บ ข้อมูล	ฐานกฎหมาย ที่ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะ จัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		8) ลายมือชื่อผู้ เรียกร้องค่าสินไหม ทดแทนหรือผู้ที่ เกี่ยวข้องในการ พิจารณาจ่าย สินไหมทดแทน 9) รายละเอียด ความเสียหายซึ่ง อาจมีข้อมูล เกี่ยวข้องหรือ เชื่อมโยงไปถึง ข้อมูลส่วนบุคคล 10) ข้อมูลบัญชี ธนาคารเพื่อจ่ายค่า สินไหมทดแทน <u>ข้อมูลส่วนบุคคลที่</u> <u>มีความอ่อนไหว</u> 1) ข้อมูลการ เจ็บป่วย/การ รักษา/การเกิดเหตุ									

กิจกรรม	วัตถุประสงค์ การเก็บข้อมูล	การเก็บรวบรวม			ระยะเวลา				การเปิดเผยข้อมูล		
		ประเภทของข้อมูล ส่วนบุคคล	ช่องทางการเก็บ ข้อมูล	ฐานกฎหมาย ที่ไม่ต้องขอ ความยินยอม	ระยะเวลา เริ่มต้น	การ ปรับปรุง แก้ไข	ระยะเวลา การเก็บ ข้อมูล	การจัดการหลัง สิ้นสุดระยะ จัดเก็บ	ภายในบริษัท	ภายนอกบริษัท (ในประเทศ)	ภายนอกบริษัท (ต่างประเทศ)
		2) ข้อมูลประวัติ อาชญากรรม เช่น บันทึกประจำวัน สำนวนการ สอบสวน หรือ เอกสารทางคดี เป็นต้น 3) ข้อมูลทางนิติ วิทยาศาสตร์ เช่น ชั้นสูตรพลิกศพ เป็นต้น									