



แนวปฏิบัติตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ว่าด้วย ธุรกิจโรงแรมและที่พัก

ฉบับปรับปรุง ตุลาคม 2566

จัดทำโดย	PDPA Thailand
สนับสนุนโดย	สมาคมโรงแรมไทย (Thai Hotel Association: THA) สมาคมธุรกิจการท่องเที่ยวภูเก็ต (Phuket Tourist Association: PTA) คณะกรรมการการท่องเที่ยว สถาบันบัณฑิตพัฒนบริหารศาสตร์ (GSTM) สมาพันธ์เอสเอ็มอีไทย สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA) สถาบันพัฒนาและทดสอบทักษะดิจิทัล
ที่ปรึกษา	คุณมาริสสา สุโกศล หนุนภักดี นายกสมาคมโรงแรมไทย (THA) นายธเนศ ดันติพิริยะกิจ นายกสมาคมธุรกิจการท่องเที่ยวภูเก็ต (PTA) ผศ.ดร.ไพฑูรย์ มนต์พานทอง คณบดีคณะกรรมการจัดการการท่องเที่ยว สถาบันบัณฑิตพัฒนบริหารศาสตร์ ดร.อุดมธิปก ไพรเกษตร เลขธิการสมาพันธ์เอสเอ็มอีไทย อาจารย์สุกฤษ โภยอัครเดช เลขธิการสมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA)
ผู้แต่ง	อาจารย์ดวงดาว สำนองสุข อาจารย์ณัฐ ธนวนกุล อาจารย์มยุรี ชวนชม อาจารย์ก่อพล ฐานะวุฒม์ อาจารย์ไพศาล สามีภักดิ์
วันที่เผยแพร่	27 กรกฎาคม 2566 20 กันยายน 2566 4 ตุลาคม 2566
เวอร์ชัน	เวอร์ชันที่ 2 ปรับแก้ไขล่าสุด วันที่ 30 สิงหาคม พ.ศ.2566 เวอร์ชันที่ 3 ปรับแก้ไขล่าสุด วันที่ 20 กันยายน พ.ศ.2566 เวอร์ชันที่ 4 ปรับแก้ไขล่าสุด วันที่ 2 ตุลาคม พ.ศ.2566

ข้อปฏิเสธความรับผิดชอบ (Disclaimer)

แนวปฏิบัติที่แนบมาไม่ได้มีสถานะทางกฎหมายเหมือนกับกฎหมาย กฎ ระเบียบ หรือข้อบังคับของทางราชการ ฉะนั้น ในทางปฏิบัติแล้ว แม้ไม่ได้ปฏิบัติตามแนวปฏิบัติก็ไม่ได้มีผลเป็นการนำมาซึ่งความรับผิดตามกฎหมายแต่ประการใด เว้นแต่ข้อห้ามที่ฝ่าฝืนนั้นจะได้รับการกำหนดเอาไว้ในกฎหมาย กฎ ระเบียบ หรือข้อบังคับของทางราชการ ทั้งนี้ ที่ปรึกษาและผู้แต่งของแนวปฏิบัตินี้ ไม่ได้ให้การรับรองหรือรับประกันใด ๆ ถึงความถูกต้องครบถ้วนของเนื้อหาของงานนี้ และผู้แต่งขอปฏิเสธอย่างชัดเจนว่าไม่ได้ให้การรับรองหรือรับประกันใด ๆ ทั้งสิ้นต่อเนื้อหาของงานนี้ โดยขอแนะนำที่ปรากฏในงานนี้อาจไม่เหมาะสมต่อสถานการณ์บางลักษณะ และหากมีการอ้างอิงใด ๆ ถึงงานนี้ไม่ว่าในรูปแบบใด ผู้แต่งขอปฏิเสธอย่างชัดเจนไม่ให้การรับรองหรือการรับประกันการอ้างอิงนั้น การรับรองใด ๆ ที่อาจมีขึ้น ต้องออกเป็นหนังสือโดยผู้แต่ง

ชื่อสถานประกอบการ โรงแรม กลุ่มธุรกิจ หรือบุคคลที่ได้หยิบยกในแนวปฏิบัตินี้ มิใช่มีวัตถุประสงค์เพื่อประโยชน์ทางการค้าหรือประโยชน์อื่นใด แต่เป็นการหยิบยกเป็นกรณีศึกษาและกรณีตัวอย่างประกอบข้อกฎหมายและข้อกำหนดต่าง ๆ เพื่อนำไปสู่ความเข้าใจทฤษฎีและการปฏิบัติจริงที่ทำให้ผู้ที่นำไปใช้หรือนำแนวทางนี้ไปพิจารณาได้จัดแจ้ง ทั้งนี้ ข้อมูลถูกนำมาจากแหล่งข้อมูลที่มีการเผยแพร่ไว้ต่อสาธารณชนก่อนหน้านี้แล้ว

คำนิยาม

จากการทำบันทึกข้อตกลงความร่วมมือ (Memorandum of Understanding) ระหว่างสถาบันบัณฑิตพัฒนบริหารศาสตร์กับสมาพันธ์เอสเอ็มอีไทย ถือเป็นจุดเริ่มต้นที่ทำให้คณะกรรมการจัดการการท่องเที่ยวได้ทำความร่วมมือกับ PDPA Thailand ในการจัดทำแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ว่าด้วยธุรกิจโรงแรมที่พัก ผ่านการสร้างกระบวนการการมีส่วนร่วมของภาคีเครือข่าย ไม่ว่าจะเป็นสมาคมโรงแรมไทย สมาคมส่งเสริมการท่องเที่ยวภูมิภาคเอเชียและแปซิฟิก (ประจำประเทศไทย) คณะกรรมการจัดการการท่องเที่ยว รวมถึงตัวแทนผู้ประกอบการโรงแรมที่พัก โดยมี PDPA Thailand เป็นเจ้าภาพหลักในฐานะที่เป็นผู้เชี่ยวชาญ และคณะกรรมการจัดการการท่องเที่ยวในฐานะผู้ประสานงานให้เกิดความร่วมมือระหว่างภาคีต่างๆ ที่เกี่ยวข้อง โดยมีการจัดประชุมกลุ่มย่อยระหว่างผู้ที่เกี่ยวข้องในธุรกิจโรงแรมที่พักจำนวน 2 ครั้ง จนในที่สุดแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ว่าด้วยธุรกิจโรงแรมที่พักได้เสร็จสมบูรณ์ และได้มีการจัดอบรมให้กับผู้ประกอบการธุรกิจโรงแรมที่พัก

ธุรกิจโรงแรมที่พักเป็นองค์ประกอบที่มีความสำคัญอย่างยิ่งในอุตสาหกรรมการท่องเที่ยว โดยได้สร้างงาน สร้างรายได้ให้กับประเทศเป็นลำดับต้น ๆ เมื่อเปรียบเทียบกับธุรกิจอื่น ๆ ในอุตสาหกรรมการท่องเที่ยว จากการที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ถูกสร้างขึ้นและมีผลบังคับใช้อย่างเป็นทางการเพื่อสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ของเจ้าของข้อมูลส่วนบุคคล จึงเป็นความท้าทายสำหรับผู้ประกอบการธุรกิจโรงแรมที่พักที่ต้องเรียนรู้ ทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด

ในนามของคณะกรรมการจัดการการท่องเที่ยว สถาบันบัณฑิตพัฒนบริหารศาสตร์ (นิด้า) ขอขอบคุณทาง PDPA Thailand โดยเฉพาะ ดร.อุดมธิปก ไพรเกษตร และ อาจารย์สุกฤษ โภยอัครเดช ที่เป็นผู้จัดทำแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ว่าด้วยธุรกิจโรงแรมที่พัก ซึ่งเป็นประโยชน์อย่างยิ่งในการนำไปใช้เป็นแนวทางในการคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ประกอบการโรงแรมที่พัก

ผู้ช่วยศาสตราจารย์ ดร.ไพฑูรย์ มนต์พานทอง
คณบดีคณะกรรมการจัดการการท่องเที่ยว
สถาบันบัณฑิตพัฒนบริหารศาสตร์ (นิด้า)

คำนิยม

จากการที่รัฐบาลได้มีการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเต็มรูปแบบ ในวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมานั้น ต้องยอมรับว่ากรอบความคิดในเรื่องข้อมูลส่วนบุคคลยังไม่แพร่หลายในธุรกิจโรงแรม กลุ่มโรงแรมที่บริหารโดยเซกเตอร์ต่างชาติอาจจะคุ้นเคยกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation : GDPR) แต่ภาคธุรกิจโรงแรมในประเทศไทยประกอบด้วยโรงแรมหลายขนาด ทั้งกลุ่มโรงแรมที่บริหารจัดการเองและกลุ่มโรงแรมเอสเอ็มอี ยังต้องการเวลาทำความเข้าใจและปรับการทำงานภายในองค์กร ซึ่งในระยะเวลาที่ผ่านมา ทางสมาคมโรงแรมไทยได้หารือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในเรื่องนี้และได้ร่วมทำแนวทางปฏิบัติเบื้องต้นให้กับโรงแรมแล้ว

อย่างไรก็ตาม รายละเอียดของกฎหมายและแนวทางปฏิบัติสำหรับแต่ละแผนกในโรงแรมมีหลากหลายมาก จึงขอขอบคุณสถาบันบัณฑิตพัฒนบริหารศาสตร์ (นิด้า) และบริษัท พีดีพีเอ (ไทยแลนด์) จำกัด (สำนักงานใหญ่) ที่จัดทำ “แนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ว่าด้วยธุรกิจโรงแรมและที่พัก” อย่างละเอียด ข้อมูลเหล่านี้ค่อนข้างละเอียดอ่อนและจะมีประโยชน์อย่างยิ่งที่จะสนับสนุนให้โรงแรมสามารถปฏิบัติตามข้อกำหนดของกฎหมาย ไม่เพียงโรงแรมที่เป็นสมาชิกของสมาคมโรงแรมเท่านั้นที่จะได้ประโยชน์ แต่โรงแรมทุกแห่งไม่ว่าจะเป็นโรงแรมใหญ่หรือเอสเอ็มอีก็จะได้รับประโยชน์จากแนวปฏิบัติเล่มนี้เช่นกัน

สมาคมโรงแรมไทยและสมาชิกรู้สึกได้รับเกียรติอย่างยิ่งที่ได้มีส่วนร่วมในการจัดทำแนวทางฉบับนี้และขอชื่นชมผู้เกี่ยวข้องทุกคนที่ได้ร่วมมือกันทำงานสำเร็จ มา ณ ที่นี้ด้วย

มาริสสา สุโกศล หนุนภักดี

นายกสมาคมโรงแรมไทย

(Thai Hotels Association: THA)



เมื่อประเทศไทยได้กำหนดให้มีการใช้ PDPA หรือ Personal Data Protection Act ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคล มาบังคับใช้เต็มรูปแบบเมื่อเดือนมิถุนายน 2565 ที่ผ่านมา โดยมีรายละเอียดข้อกำหนดให้หน่วยงานทั้งรัฐและเอกชนต่าง ๆ รวมถึงอุตสาหกรรมการท่องเที่ยว ที่มีการเก็บรวบรวม ใช้เปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามมาตรการต่าง ๆ เพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวให้แก่ผู้เข้าพัก ลูกค้า คู่ค้า ลูกจ้าง

PDPA Thailand ในฐานะหน่วยงานชั้นนำที่มีพันธกิจในการวิจัย และสร้างองค์ความรู้ รวมทั้งเผยแพร่ประเด็นและข้อเสนอแนะด้านการคุ้มครองข้อมูลส่วนบุคคลที่เป็นประโยชน์ต่อสังคม ตระหนักถึงผลกระทบของ PDPA ต่ออุตสาหกรรมการท่องเที่ยว โดยเฉพาะภาคธุรกิจโรงแรม จึงเห็นความสำคัญและความจำเป็นที่ควรมีการศึกษาวิจัยเพื่อสร้างแนวปฏิบัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล ว่าด้วยธุรกิจโรงแรมและที่พัก เพื่อรองรับการมีผลบังคับใช้ของ PDPA (Personal Data Protection Act B.E. 2562) รวมถึงเพื่อให้ผู้ประกอบการธุรกิจโรงแรมและที่พักนั้น สามารถนำไปเป็นแนวทางการดำเนินการพื้นฐาน ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างถูกต้อง

PDPA Thailand หวังเป็นอย่างยิ่งว่า “แนวปฏิบัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล ว่าด้วยธุรกิจโรงแรมและที่พัก” ซึ่งเป็นผลงานของสถาบันชั้นนำนี้จะก่อให้เกิดการตระหนักรู้และสร้างการตื่นตัวในอุตสาหกรรมโรงแรม รวมทั้งเกิดประโยชน์แก่ผู้ประกอบการและลูกจ้างของไทย ที่จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้จริง

เอกสารฉบับนี้จะเกิดขึ้นไม่ได้เลย หากไม่ได้รับการสนับสนุนในความคิดเห็นและข้อเสนอแนะตลอดจนความร่วมมืออย่างดียิ่งในประเด็นปัญหา จากคุณมาริส สุโกศล หนูนภักดี นายกสมาคมโรงแรมไทย นายธนศ ตันติพิริยะกิจ นายกสมาคมธุรกิจการท่องเที่ยวภูเก็ต (PTA) ผู้ช่วยศาสตราจารย์ ดร.ไพฑูรย์ มนต์พานทอง คณบดีคณะการจัดการการท่องเที่ยว (Graduate School of Tourism Management: GSTM) สถาบันบัณฑิตพัฒนบริหารศาสตร์ ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย อาจารย์สุกฤษฎ์ โภยอัครเดช เลขาธิการสมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA) และคณาจารย์ที่ปรึกษาจากสถาบันพัฒนาและทดสอบทักษะดิจิทัล DDTI ได้แก่ อาจารย์ดวงดาว สำนองสุข อาจารย์ณัฏฐ์ ธนวนกุล อาจารย์มยุรี ชวนชม อาจารย์ก่อพล ฐานะวุฒม์ และอาจารย์ไพศาล สามิภักดิ์ โดยได้มีความคิดเห็นและข้อเสนอแนะเพิ่มเติมในการปรับปรุงให้เอกสารมีความสมบูรณ์มากขึ้น

คณะผู้จัดทำ

PDPA THAILAND

7 กรกฎาคม 2566

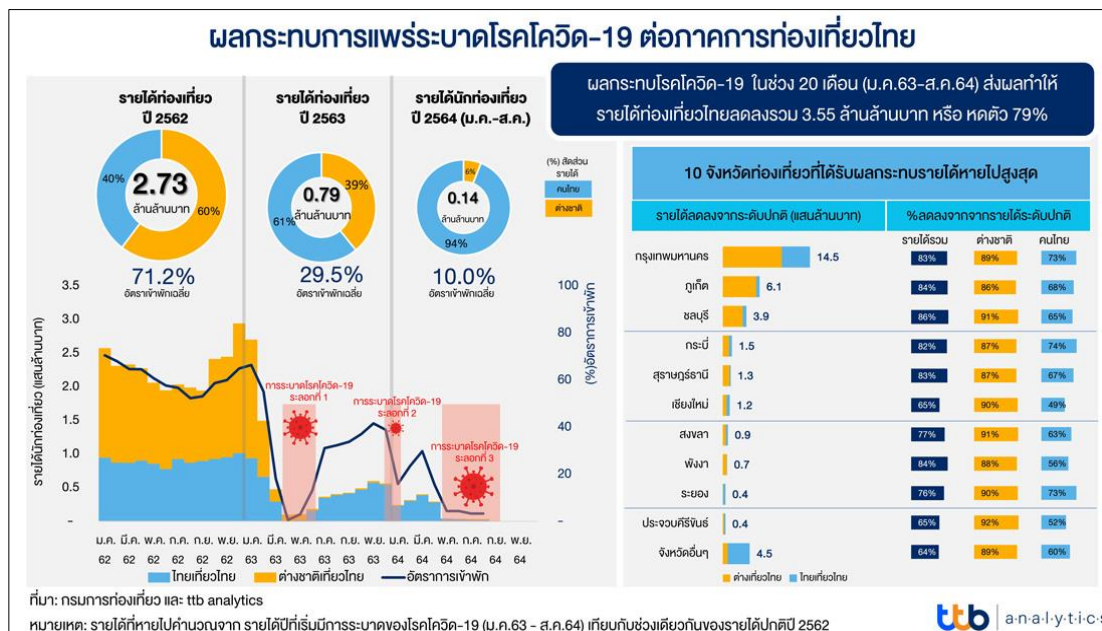
สารบัญ

	หน้า
คำนิยม	ค
สารบัญ.....	ฉ
1.บทนำ.....	1
2. แนวคิดและหลักการพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.....	3
2.1 ที่มาและความสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล	3
2.2 เจตนารมณ์ของกฎหมาย	3
2.3 ขอบเขตการบังคับใช้.....	3
2.4 นิยามข้อมูลส่วนบุคคล	6
2.5 บุคคลที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	7
2.6 หลักการในการประมวลผลข้อมูลส่วนบุคคล	14
2.7 ฐานทางกฎหมาย (Lawful Basis)	15
2.8 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ “ไม่ใช่” จากเจ้าของข้อมูลโดยตรง	19
2.9 การใช้ หรือการเปิดเผยข้อมูล	20
2.10 การส่งหรือโอนข้อมูลไปต่างประเทศ.....	20
2.11 สิทธิของเจ้าของข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล.....	20
2.12 บทกำหนดโทษ.....	23
3. กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับธุรกิจโรงแรมและที่พัก.....	25
3.1 ภาพรวมธุรกิจโรงแรมและที่พัก.....	25
3.2 วงจรการให้บริการผู้เข้าพักโรงแรม (Guest Cycle) และวงจรชีวิตข้อมูลส่วนบุคคล (Data Life Cycle)	26
3.2.1 กระบวนการการรับการจอง (Reservation Process)	29
3.2.2 กระบวนการการรับที่สนามบิน (Pick-up service activity).....	32
3.2.3 กระบวนการลงทะเบียนเข้าพัก (Checked-in Process)	34
3.2.4 กระบวนการนำส่งบันทึกลงในทะเบียนผู้เข้าพักหรือเอกสาร ร.ร. 4 ให้กับกรมการปกครอง.....	36
3.2.5. กระบวนการนำส่ง ตม. 30 ให้สำนักงานตรวจคนเข้าเมือง	38
3.2.6 กระบวนการการใช้กล้องวงจรปิด (CCTV Using Process)	40
3.2.7 กระบวนการการเปิดสมาชิก (Hotel Member Process)	43
3.2.8 กระบวนการการรับชำระค่าบริการโรงแรม (Hotel Payment Process)	44

3.2.9 กระบวนการการขายทัวร์ (Tour Desk Process)	45
3.2.10 กระบวนการ การให้บริการสปา (Spa Service Process)	47
3.2.11 กระบวนการการทำการตลาดหลัง Check out.....	49
3.3 กรณีศึกษา.....	51
3.3.1. กรณีศึกษา โรงแรม Marriott ถูกขโมยข้อมูลของผู้เข้าพักผู้เข้าพักกว่าจำนวน 339 ล้านคน.....	51
3.3.2. กรณีศึกษา เว็บไซต์รับจองที่พัก Booking.com ถูกปรับเนื่องจากไม่รายงานการละเมิดข้อมูลภายในระยะเวลาที่กำหนด.....	51
3.3.3. กรณีศึกษา โรงแรม Accor ถูกปรับ เพราะทำผิดหลักการขอความยินยอม	52
3.3.4. กรณีศึกษา บริษัท TAXA 4x35 ถูกปรับ เพราะไม่ลบข้อมูลลูกค้าเมื่อสิ้นสุดการใช้งาน	53
4. บทบาทโรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคล	54
5. ขั้นตอนการเตรียมความพร้อมขององค์กร	57
ภาคผนวก.....	60

1.บทนำ

ในช่วงหลายปีที่ผ่านมา สถานการณ์โควิด (COVID-19) ได้ส่งผลกระทบต่ออุตสาหกรรมในทุกภาคส่วนของประเทศไทย และเศรษฐกิจทั่วโลก โดยเฉพาะอย่างยิ่งภาคธุรกิจการท่องเที่ยว ซึ่งถือว่าเป็นอุตสาหกรรมสำคัญหลักที่สร้างรายได้ให้กับประเทศไทย อันจะเห็นได้จากสถิติจำนวนนักท่องเที่ยวที่ลดลง จากการท่องเที่ยวแห่งประเทศไทย (ททท.) และ TTB Analytics



ที่มา : <https://www.ttbbank.com/th/newsroom/detail/travel-thailand-after-unlocking>

ในปัจจุบัน อุตสาหกรรมการท่องเที่ยวหลังสถานการณ์โควิด มีการคาดการณ์ว่าจะดีขึ้นมากกว่า 20% จากการคาดการณ์ของการท่องเที่ยวแห่งประเทศไทย (ททท.) ซึ่งเมื่อสถานการณ์ด้านการท่องเที่ยวของประเทศไทยดีขึ้นย่อมส่งผลให้จำนวนคนที่เข้ามาท่องเที่ยวก็จะมีมากขึ้นตามมา ไม่ว่าจะเป็นนักท่องเที่ยวที่เป็นคนในประเทศเอง หรือนักท่องเที่ยวจากต่างประเทศ

นอกจากนี้ ประเทศไทยได้มีการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเป็นทางการในวันที่ 1 มิถุนายน 2565 รวมถึงกฎหมายฉบับรองที่ทยอยออกมานั้น จากเหตุดังกล่าวทำให้การคุ้มครองข้อมูลส่วนบุคคลเข้าไปมีบทบาทกับอุตสาหกรรมการท่องเที่ยวอย่างมาก เนื่องจากกระบวนการในอุตสาหกรรมมีการเก็บรวบรวมข้อมูลของบุคคลจำนวนมาก ไม่ว่าจะเป็นข้อมูลที่ได้มาจากการลงทะเบียน หรือการจองที่พัก การจองทัวร์ การจัดการจราจร เป็นต้น ซึ่งต้องมีการเก็บข้อมูลส่วนบุคคลจำนวนมาก

นอกจากกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะกระทบต่อคนภายในประเทศแล้ว ยังมีผลต่อนักท่องเที่ยวที่เดินทางมาจากต่างประเทศด้วย เนื่องจากการที่เราเก็บข้อมูลส่วนบุคคลจากต่างประเทศนั้น

โดยเฉพาะข้อมูลส่วนบุคคลในภาคพื้นยุโรป กฎหมายที่เราควรนำมาพิจารณาเพิ่มเติมคือ GDPR หรือ General Data Protection Regulation เนื่องจากมีบางกิจกรรมที่เราได้มีการเก็บข้อมูลจากพลเมืองยุโรป และนำมาประมวลผล ทำให้อุตสาหกรรมโรงแรมเป็นอุตสาหกรรมที่ต้องให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล

ในอุตสาหกรรมการท่องเที่ยวประกอบไปด้วยธุรกิจที่มาจากหลายภาคส่วน ตั้งแต่ ธุรกิจนำเที่ยวและมัคคุเทศก์ ธุรกิจโรงแรมและที่พัก ธุรกิจการจัดประชุมและนิทรรศการ ธุรกิจร้านขายของที่ระลึก ธุรกิจรับ-ส่งรถยนต์บริการ ธุรกิจสปาหรือสถานบริการสุขภาพ เป็นต้น โดยในแนวปฏิบัติฉบับนี้จะกล่าวถึง **เฉพาะธุรกิจโรงแรมและที่พักในที่เกี่ยวข้องกับแขกในสถานะผู้เข้าพักเท่านั้น**

ในการวิเคราะห์กระบวนการที่เกี่ยวข้องกับการประมวลผลข้อมูล เพื่อให้ครอบคลุม เราจะต้องพิจารณาตั้งแต่การเก็บรวบรวม การเก็บรักษา การใช้เปิดเผย และการทำลายข้อมูลส่วนบุคคล เพื่อให้สามารถเห็นภาพทั้งกระบวนการ สามารถปิดช่องโหว่ (Gap) อันก่อให้เกิดความเสี่ยง (Risk) ในการรั่วไหลหรือละเมิดข้อมูลส่วนบุคคลได้ ซึ่งธุรกิจโรงแรมและที่พักจะมีกระบวนการหลัก ๆ ดังต่อไปนี้

- 1) การค้นหาที่พัก: เป็นกระบวนการตั้งแต่นักท่องเที่ยวสนใจจองห้องพักผ่านทางช่องทางต่าง ๆ เช่น Line OA Website โรงแรม หรือช่องทางการติดต่อต่าง ๆ หรือเป็นกรณีที่นักท่องเที่ยวตัดสินใจไปจองผ่าน Online Travel Agency (OTA)
- 2) การเข้าพัก: เป็นกระบวนการเริ่มตั้งแต่นักท่องเที่ยวเช็คอินเข้าที่พักจนกระทั่งเช็คเอาท์กลับ โดยในกระบวนการดังกล่าวนักท่องเที่ยวจะต้องมีการกรอกแบบฟอร์มต่าง ๆ ตัวอย่างเช่น รร. 4 หรือ ตม. 30 สำหรับนักท่องเที่ยวต่างชาติตามแต่กรณี รวมไปถึงช่วงเวลาที่ลูกค้าใช้บริการต่าง ๆ ภายในโรงแรม เช่น บริการร้านอาหาร บริการสระว่ายน้ำ บริการห้องออกกำลังกาย บริการสปา หรือบริการการท่องเที่ยวในพื้นที่ เช่น ทริปวันวิง หรือทริปครึ่งวันไปดำน้ำเกาะต่าง ๆ ในบริเวณใกล้เคียง เป็นต้น
- 3) การเช็คเอาท์: ซึ่งเป็นการที่นักท่องเที่ยวชำระเงินผ่านทางช่องทางต่าง ๆ มากมาย ไม่ว่าจะเป็นการชำระเงินโดยตรงกับโรงแรม หรือผ่านช่องทางอื่น ๆ
- 4) การติดตามหลังเช็คเอาท์: ทีมการตลาดของโรงแรมที่อาจมีการส่งอีเมลหรือจดหมายขอบคุณ หรือส่งรูปที่ระลึกทางอิเล็กทรอนิกส์ไปให้ลูกค้าพร้อมแนบคู่มือบางส่วนลดสำหรับการเข้าพักครั้งต่อไป

การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องสำคัญที่ผู้ประกอบการโรงแรมในฐานะ “ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) ต้องให้ความสำคัญ นอกจากจะเป็นการปฏิบัติตามกฎหมายแล้ว การที่ผู้ประกอบการให้ความสำคัญถึงความเป็นส่วนตัวของนักท่องเที่ยว ย่อมส่งผลให้เกิดความไว้วางใจกับนักท่องเที่ยวในฐานะเจ้าของข้อมูลส่วนบุคคล อันส่งผลดีต่อผู้ประกอบการโดยตรง ซึ่งได้แก่ความน่าเชื่อถือ ชื่อเสียงอีกด้วย

2. แนวคิดและหลักการพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2.1 ที่มาและความสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ภายหลังจากที่สหภาพยุโรป (European Union: EU) ได้มีการประกาศใช้ General Data Protection Regulation หรือ GDPR เมื่อวันที่ 24 พฤษภาคม พ.ศ. 2559 โดยมีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม พ.ศ. 2561 เป็นต้นมา 1 ปีต่อมา ประเทศไทยได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) โดยประกาศในราชกิจจานุเบกษา ในวันที่ 27 พฤษภาคม พ.ศ. 2562 ซึ่งมีการบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป โดยมีจุดประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชน รวมถึงมีมาตรการในการดูแลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ซึ่งในนี้นอกจากนักท่องเที่ยวแล้ว ยังรวมไปถึงพนักงานบุคลากรของโรงแรมด้วยเช่นกัน

บทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่บทบัญญัติจะมุ่งเน้นสร้างความตระหนักรู้ การทบทวน และกลไกในการพิจารณาเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต่าง ๆ เพื่อให้การกระทำใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวส่วนตัวภายใต้หลักการของกฎหมาย

2.2 เจตนารมณ์ของกฎหมาย

ในปัจจุบันมีการละเมิดข้อมูลส่วนบุคคลเป็นจำนวนมาก อีกทั้งความก้าวหน้าและวิวัฒนาการของระบบเทคโนโลยีที่ทำให้การล่วงละเมิดเป็นไปได้โดยง่าย และรวดเร็ว ยกตัวอย่างกรณี 9near กับข้อมูลประชากร 55 ล้านคนที่มีการหลุดรอดมาจากหน่วยงานรัฐ หรือในกรณีศึกษาจากโรงแรม Marriott ที่ถูกขโมยข้อมูลก็ตาม (สามารถอ่านเป็นกรณีศึกษาได้ในหัวข้อ 3.3 กรณีศึกษา) เห็นได้ชัดว่าปัจจุบันข้อมูลส่วนบุคคลถูกละเมิดได้โดยง่าย โดยข้อมูลเหล่านี้มีความสำคัญมากทั้งนี้หากไม่มีการปกป้องคุ้มครองดูแลก็อาจทำให้เกิดความเสียหายแก่ประชาชน ซึ่งในธุรกิจการท่องเที่ยวข้อมูลของนักท่องเที่ยวมีความสำคัญมากดังที่กล่าวในส่วนของบทนำ ด้วยเหตุนี้เองประเทศไทยจึงได้มีการจัดทำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นมาตรฐานในการดูแลคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัยยิ่งขึ้น

2.3 ขอบเขตการบังคับใช้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีขอบเขตการบังคับใช้ ดังต่อไปนี้

1. กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ “ใน” ประเทศไทย ไม่ว่าจะการประมวลผลนั้น ได้กระทำในหรือนอกประเทศไทยก็ตาม เช่น โรงแรม A ตั้งอยู่จังหวัดภูเก็ต ได้เก็บข้อมูล

ชื่อ นามสกุล รวมถึงรายละเอียดการเข้าพักอื่น ๆ ของแขกคนไทยที่อยู่ในเมืองไทย หรือ แขกต่างชาติที่จองห้องพักมาจากเมืองนอก อย่างไรก็ตามโรงแรม A ในฐานะผู้ประกอบการ และผู้ควบคุมข้อมูลส่วนบุคคล เป็นนิติบุคคลที่อยู่ในประเทศไทย โรงแรม A ต้องปฏิบัติตามกฎหมายฉบับนี้

2. กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ “นอก” ประเทศไทย จะใช้บังคับใช้กับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในประเทศไทย โดยการดำเนินการกระบวนการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

1) กิจกรรมการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่า จะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม เช่น โรงแรม A ตั้งอยู่ที่สเปน ได้มีการทำการตลาด โดยเสนอห้องพักลดราคาในช่วง Low Season กับนาย B ที่พำนักอยู่ในประเทศไทย ซึ่งนาย B เคยเดินทางไปใช้บริการโรงแรม A ที่สเปนมาก่อน การทำการตลาดที่เสนอราคาห้องพักลดราคาดังกล่าว เป็นการเสนอขายสินค้าหรือบริการโดยผู้ควบคุมข้อมูลที่อยู่นอกราชอาณาจักร ให้แก่เจ้าของข้อมูลซึ่งอยู่นอกราชอาณาจักร โรงแรม A ต้องพิจารณาถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

2) กิจกรรมการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศไทย เช่น โรงแรม A ที่ตั้งอยู่ประเทศสเปน ได้มีการติดตามพฤติกรรมการค้นหาโรงแรมของนาย B (ซึ่งเคยเข้าพักกับโรงแรม A และได้มีการดาวน์โหลดแอปพลิเคชันสมาชิกโรงแรม) การติดตามพฤติกรรมดังกล่าว เกิดกับแขกที่เป็นเจ้าของข้อมูลส่วนบุคคลที่พำนักอยู่ในประเทศไทย โดยโรงแรม A ที่อยู่ประเทศสเปนนั้น ต้องพิจารณาถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

อย่างไรก็ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่บังคับแก่กิจการ องค์กร หรือกระบวนการบางกลุ่ม ดังต่อไปนี้

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกระบวนการในครอบครัวของบุคคลนั้นเท่านั้น ตัวอย่างเช่น พ่อแม่เก็บข้อมูลส่วนบุคคลของลูกที่ทะเลาะวิวาทถูกตี เป็นต้น
- การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ เช่น การดำเนินการตรวจสอบของคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เป็นต้น
- กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น ทั้งนี้ต้องย้าว่าเป็นไปตามจริยธรรมหรือวิชาชีพเท่านั้น หากไม่ได้เป็นไปตามหลักวิชาชีพก็จะไม่ได้รับการยกเว้น

- สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภา ต้องดำเนินการไปตามหน้าที่และอำนาจของสภาผู้แทนราษฎรเท่านั้น ดังนั้นหากผู้แทนดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลนอกเหนือจากอำนาจดังกล่าว ย่อมไม่ได้รับการยกเว้น
- การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี
- การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากนี้ ได้มีกฎหมายลำดับรองกำหนดเพิ่มเติมให้ในบางกรณีว่า ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อาจไม่ต้องปฏิบัติตาม PDPA ในหมวด 2 เรื่องการคุ้มครองข้อมูลส่วนบุคคลและหมวด 3 เรื่องสิทธิของเจ้าของข้อมูล หากเข้าหลักเกณฑ์ตามที่กฎหมายกำหนดไว้ ซึ่งก็คือ “พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บางส่วนมาใช้บังคับ พ.ศ.2566”

โดยกฎหมายลำดับรองฉบับนี้ ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลทั้งภาครัฐและภาคเอกชน ได้รับยกเว้นในการปฏิบัติตามหมวด 2 และหมวด 3 ในกรณีดังต่อไปนี้

(1) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการทุจริต เช่น ป.ป.ช. ป.ป.ท. หรือหน่วยงานรัฐที่คณะกรรมการประกาศกำหนด

(2) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจาก กรมสรรพากร กรมศุลกากร หรือกรมสรรพสามิต ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีอากรและความร่วมมือระหว่างประเทศเกี่ยวกับภาษี

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้ และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(3) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากองค์กรปกครองส่วนท้องถิ่น ที่คณะกรรมการประกาศกำหนด ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(4) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากสำนักเลขาธิการ คณะรัฐมนตรีเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการสถาปนาสมณศักดิ์ การแต่งตั้งหรือถอดถอนข้าราชการ บุคคลหรือคณะบุคคล ซึ่งเป็นพระราชอำนาจของพระมหากษัตริย์ หรือที่ต้องเสนอคณะรัฐมนตรี และการขอพระราชทาน หรือเรียกคืนเครื่องราชอิสริยาภรณ์ ฎีกาซึ่งมีผู้ทูลเกล้าฯถวาย หรือการขอพระราชทานพระมหากรุณาในเรื่องต่าง ๆ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(5) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจเพื่อดำเนินการตามวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญตามที่คณะกรรมการประกาศกำหนด

(6) กรณีการประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการเนรเทศ การส่งผู้ร้ายข้ามแดน ความร่วมมือระหว่างประเทศเกี่ยวกับกระบวนการยุติธรรมทางอาญา การป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ความร่วมมืออื่นทางศาล หรือกระบวนการยุติธรรมระหว่างประเทศ

(7) การประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐตามพระราชกฤษฎีกานี้ บรรดาที่มีกฎหมายหรือพระราชกฤษฎีกานี้ให้อำนาจในการขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามหน้าที่และอำนาจที่กฎหมายกำหนดไว้ หน่วยงานของรัฐซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมได้รับการยกเว้นเช่นเดียวกัน

แม้ว่าผู้ควบคุมข้อมูลส่วนบุคคลตามที่ระบุไว้ในพระราชกฤษฎีกาข้างต้นจะได้รับการยกเว้นการปฏิบัติตาม PDPA ในหมวด 2 และ 3 แต่เขาก็ยังคงมีหน้าที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด

2.4 นิยามข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแบ่งเป็น 2 ประเภท ได้แก่

1. ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล ชื่อเล่น หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เลขหนังสือเดินทาง ข้อมูลการเข้าพัก เลขบัญชี เลขบัตรเครดิต เป็นต้น

อย่างไรก็ดี ข้อมูลต่อไปนี้ไม่เป็นข้อมูลส่วนบุคคล เช่น ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น ชื่อโรงแรม ที่อยู่ของโรงแรม เลขทะเบียนนิติบุคคลของโรงแรม หมายเลขโทรศัพท์ของที่ทำงาน

ที่อยู่อีเมล (E-mail address) ของโรงแรม เช่น info@HotelABC.co.th ข้อมูลนิรนาม (Anonymous Data) เป็นต้น

2. ข้อมูลส่วนบุคคลละเอียดอ่อน (Sensitive Data) หรือข้อมูลส่วนบุคคลชนิดพิเศษ (Special Categories of Personal Data) หมายถึง ข้อมูลส่วนบุคคลตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เช่น อาการแพ้อาหารทะเล (ข้อมูลสุขภาพ) โรคหัวใจ (ข้อมูลสุขภาพ) ข้อมูลความพิการทางการได้ยิน (ข้อมูลความพิการ) เป็นต้น

2.5 บุคคลที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลที่ข้อมูลส่วนบุคคลสามารถระบุตัวตนหรือชี้แสดงไปที่ตัวบุคคลเขาเอง โดยเจ้าของข้อมูลส่วนบุคคลหมายถึงบุคคลธรรมดาที่ยังมีชีวิตอยู่เท่านั้นโดยไม่รวมถึงนิติบุคคล (Juristic Person) เจ้าของข้อมูลส่วนบุคคล ได้แก่ บุคคลดังต่อไปนี้

- 1) บุคคลที่บรรลุนิติภาวะ หมายถึง บุคคลที่มีอายุตั้งแต่ 20 บริบูรณ์ขึ้นไป และหมายถึงบุคคลที่มีการสมรส เนื่องจากกฎหมายได้มีบัญญัติไว้ว่าบุคคลจะบรรลุนิติภาวะได้ในกรณี ได้แก่ อายุถึงตามที่กฎหมายกำหนด และการสมรส ซึ่งเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะสามารถให้ความยินยอมได้ด้วยตนเอง
- 2) บุคคลที่เป็นผู้เยาว์ หมายถึง บุคคลที่อายุต่ำกว่า 20 ปีบริบูรณ์ และไม่ได้บรรลุนิติตามกฎหมายซึ่งได้แก่การสมรส ซึ่ง การให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ เว้นแต่เข้าข้อยกเว้นตามกฎหมาย
- 3) บุคคลเสมือนไร้ความสามารถ หมายถึง บุคคลที่ศาลสั่งให้เป็นคนเสมือนไร้ความสามารถเนื่องจากมีกายพิการหรือมีจิตฟั่นเฟือนไม่สมประกอบ หรือประพฤติดุร้ายสุรุยเสเพลเป็นอาชญา หรือติดสุรายาเมา หรือมีเหตุอื่นใดทำนองเดียวกันนั้น จนไม่สามารถจะจัดทำกรงานโดยตนเองได้ หรือจัดกิจการไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือครอบครัว ซึ่งการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้พิทักษ์ก่อน
- 4) บุคคลไร้ความสามารถ หมายถึง บุคคลที่ศาลสั่งให้เป็นคนไร้ความสามารถ การให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้อนุบาลก่อน

2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคล ซึ่งในบริบทแนวปฏิบัติฉบับนี้คือตัวกิจการ “โรงแรม” ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ไม่ได้จำกัดแต่เฉพาะในภาคเอกชนเท่านั้น แต่ยังรวมถึงโรงแรมที่อยู่ภายใต้การกำกับของมหาวิทยาลัย เช่น โรงแรมดุสิตเพลส ซึ่งอยู่ภายใต้การกำกับดูแลของสำนักกิจการพิเศษ มหาวิทยาลัยสวนดุสิต

ก็ถือว่าเป็นสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

- 1) เก็บรวบรวม ใช้ เปิดเผย ให้เป็นไปตามกฎหมาย หมายถึง ต้องมีฐานทางกฎหมายรองรับ ดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลไม่ว่าจะเป็น นักท่องเที่ยวในฐานะลูกค้า หรือแขก ได้ทราบ และต้องมีการขอความยินยอมในการเก็บข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้นตามฐานของกฎหมาย ในหัวข้อ 2.7 ฐานทางกฎหมาย รวมถึงดำเนินการด้านเอกสาร เพื่อให้ลูกค้า หรือแขก ในฐานะเจ้าของข้อมูลส่วนบุคคลมั่นใจว่า โรงแรมมีกระบวนการคุ้มครอง และรักษาข้อมูลส่วนบุคคลของแขกที่ได้มาตรฐาน
- 2) ดำเนินการรองรับการใช้สิทธิจากลูกค้าหรือแขกผู้เข้าพักในฐานะ เจ้าของข้อมูลส่วนบุคคล หมายถึง เมื่อมีคำร้องขอจากลูกค้าหรือแขก ทางผู้ประกอบการโรงแรมจะต้องดำเนินการตอบสนองการใช้สิทธิของลูกค้า/แขกโดยไม่ชักช้า ทั้งดำเนินการตามคำขอหรือการปฏิเสธการร้องขอ
- 3) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- 4) จัดให้มีมาตรการป้องกันไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น เช่น มีการโอนข้อมูลส่วนบุคคลให้ บริษัท Cloud Service หรือ บริษัทการตลาดอื่น ๆ ที่มีสถานะเป็นผู้ประมวลผลข้อมูล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ถูกต้องตามกฎหมาย
- 5) จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนแขกได้อีกต่อไปผู้ประกอบการโรงแรมต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น
- 6) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โรงแรมต้องแจ้งเหตุการณ์ละเมิดแก่หน่วยงานกำกับดูแล ซึ่งได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง นับแต่เมื่อทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่เมื่อมีการสอบสวน และตรวจสอบมาตรการภายในแล้ว และการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางมาตรการเยียวยาโดยไม่ล่าช้า
- 7) หน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล (Record of Processing Activities: RoPA) ผู้ประกอบการมีหน้าที่ต้องจัดทำเอกสารที่ชื่อว่า “บันทึกการประมวลผลข้อมูล” เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือ หรือระบบอิเล็กทรอนิกส์ก็ได้

- 8) จัดให้มีสัญญาการประมวลผลข้อมูล (Data Processing Agreement: DPA) หากโรงแรมมีการว่าจ้างคู่ค้าซึ่งเข้าสถานะนิยามผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว โรงแรมต้องจัดให้มีสัญญาการประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมและกำกับกับการดำเนินงานของคู่ค้าตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล
- 9) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หากลักษณะโรงแรมของผู้ประกอบการเข้าข่ายตามที่กฎหมายกำหนด ผู้ประกอบการต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสำหรับโรงแรม

3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่ง หรือ ในนามของโรงแรมซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ยกตัวอย่างเช่น โรงแรมว่าจ้างบริษัทรถยนต์ลีมูซีน (Limousine Service Company) ซึ่งเป็นธุรกิจประกอบกิจการขนส่งคนโดยสาร ให้ไปรับแขกลูกค้าพร้อมด้วยคนขับรถ จากสนามบินมาโรงแรม ซึ่งในกิจกรรมการรับส่งสนามบินนี้ บริษัทรถยนต์ลีมูซีนทำตามคำสั่งของโรงแรมจึงมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้

- 1) ประมวลผลข้อมูลส่วนบุคคลภายใต้คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกิจกรรมที่ได้รับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
- 2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม เช่นเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- 3) แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุ การละเมิดข้อมูลส่วนบุคคลที่เกิดกับผู้ประมวลผลข้อมูลส่วนบุคคล ตรงนี้ถือว่าเป็นข้อแตกต่างชัดเจนระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล โดยผู้ประมวลผลข้อมูลส่วนบุคคลหากเกิดเหตุรั่วไหลต้องดำเนินการแจ้งเหตุรั่วไหลแก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลจะแจ้งเหตุรั่วไหลกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- 4) จัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำและเก็บรักษาบันทึกการของกระบวนการการประมวลผลข้อมูลส่วนบุคคล
- 5) ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากโรงแรมนั้น โรงแรมต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

ข้อสังเกต : พนักงานในโรงแรม บริษัท ห้างร้าน ที่กระทำตามคำสั่งหรือในนามของโรงแรมไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เมื่อกิจการของผู้ประกอบการเข้าหลักเกณฑ์ตามที่กฎหมายกำหนด ผู้ประกอบการต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลซึ่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีบทบาทในธุรกิจโรงแรม ดังนี้

- 1) ให้คำแนะนำแก่บุคลากรในโรงแรม เรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- 2) คอยดูแลตรวจสอบกระบวนการทำงานให้สอดคล้องกับหลักของการคุ้มครองข้อมูลส่วนบุคคล
- 3) เป็นผู้ประสานงานหลักในกรณีที่เกิดเหตุที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เวลาเกิดปัญหา
- 4) รักษาความลับข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มา เนื่องจากการปฏิบัติหน้าที่ การสอบสวนกรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคล

กฎหมาย (มาตรา 41) ได้กำหนดให้ผู้ควบคุมและผู้ประมวลผลที่มีการประมวลผลข้อมูลส่วนบุคคลในลักษณะ 3 กรณี ดังต่อไปนี้ ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

กรณีแรก หน่วยงานรัฐที่ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (1) ได้มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งได้กำหนดรายชื่อหน่วยงานรัฐ เช่น กรมการกงสุล กรมการท่องเที่ยว กรมการขนส่งทางบก กรมพัฒนาธุรกิจการค้า กรมการปกครอง กรมการจัดหางาน สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น¹

กรณีที่สอง ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) ซึ่งได้มีการวาง

¹ สามารถดูรายชื่อหน่วยงานรัฐทั้งหมดตามประกาศได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 <https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf>

หลักเกณฑ์ที่สำคัญ กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะครบทั้ง 3 องค์ประกอบ จะต้องมีการแต่งตั้ง DPO โดยองค์ประกอบทั้งสามประการ มีดังนี้²

องค์ประกอบประการแรก การดำเนินกิจกรรมในการประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) โดยกิจกรรมหลัก หมายถึง การดำเนินการที่จำเป็นและสำคัญต่อเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล แต่ไม่รวมถึงกิจกรรมเสริมที่เป็นงานสนับสนุนในการดำเนินงานซึ่งไม่ใช่การดำเนินงานที่จำเป็นและสำคัญเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ในประกาศฯ ได้ยกตัวอย่างว่า การประมวลผลข้อมูลส่วนบุคคลของลูกค้าเพื่อให้บริการแก่ลูกค้า และบันทึกการรับบริการของลูกค้าเป็นการดำเนินการที่จำเป็นและสำคัญต่อการให้บริการรับจ้างขนส่งสินค้า หรือการประมวลผลข้อมูลส่วนบุคคลจากกล้องวงจรปิดเป็นการดำเนินการที่จำเป็นและสำคัญต่อการรับจ้างรักษาความปลอดภัย แต่ไม่รวมถึงงานสนับสนุนด้านบุคลากรและเทคโนโลยีสารสนเทศซึ่งเป็นเพียงงานสนับสนุนสำหรับการให้บริการรับจ้างขนส่งสินค้าหรือการรับจ้างรักษาความปลอดภัยให้กับสถานที่ต่าง ๆ

องค์ประกอบประการที่สอง การดำเนินกิจกรรมนั้นมีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ หมายถึง การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลักที่มีการเฝ้าติดตาม (track) เฝ้าสังเกต (monitor) วิเคราะห์ หรือทำนายพฤติกรรม ทิศนคติ หรือลักษณะเฉพาะของบุคคลอย่างเป็นระบบ (profile) และเกิดขึ้นเป็นประจำหรือปกติ (regular)

โดยในกรณีดังต่อไปนี้ จะถือเป็นกรณีที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ

- การประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์ หรือบัตรอื่นใดที่มีลักษณะเดียวกันซึ่งผู้ให้บริการสามารถตรวจสอบรายละเอียดข้อมูลการใช้งานบัตรได้

² สามารถดูรายละเอียดของประกาศฉบับนี้ได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 <https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf>

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการซึ่งเกิดเป็นปกติธุระหรือประจำ ที่มีการตรวจสอบสถานะ ประวัติ คุณสมบัติก่อนเข้าทำสัญญาหรือให้บริการเพื่อประเมินความเสี่ยงด้านต่าง ๆ เช่น การให้คะแนนเครดิต การพิจารณาเบี้ยประกันภัย การป้องกันการฉ้อฉล เป็นต้น

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาติดตามพฤติกรรม (behavioral advertising)

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้ให้บริการระบบเครือข่ายคอมพิวเตอร์หรือผู้ประกอบการกิจการโทรคมนาคม

- การประมวลผลข้อมูลส่วนบุคคลเพื่อการเฝ้าระวังและรักษาความปลอดภัยตามสถานที่ต่าง ๆ

- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

และองค์ประกอบประการสุดท้าย กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale) โดยจะพิจารณาจากปัจจัย ดังต่อไปนี้

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือสัดส่วนเจ้าของข้อมูลที่ประมวลผล เมื่อเทียบกับจำนวนเจ้าของข้อมูลทั้งหมดที่อาจเป็นไปได้

- ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่ประมวลผล

- ระยะเวลาหรือความคงอยู่ของการประมวลผลเพื่อประโยชน์ในการดำเนินกิจกรรมหลัก

- ขอบเขตการใช้ข้อมูลส่วนบุคคลขององค์กร หรือตามขนาดพื้นที่หรือจำนวนประเทศที่เกี่ยวข้องกับการประมวลผล

โดยในกรณีดังต่อไปนี้ จะถือเป็น กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale)

- การประมวลผลข้อมูลส่วนบุคคลจำนวนตั้งแต่ 100,000 รายขึ้นไป

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม ผ่านโปรแกรมค้นหาหรือสื่อสังคมออนไลน์

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานโดยปกติของบริษัท ตามกฎหมายว่าด้วยประกันชีวิตและกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้รับใบอนุญาตประกอบธุรกิจ
โทรคมนาคมแบบที่สามตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม

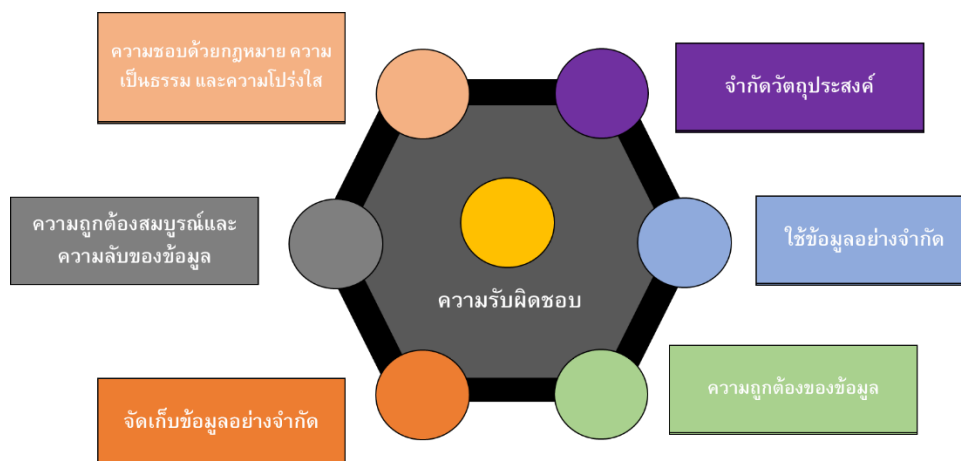
- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ดังนั้น หากผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายใดที่การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่ง
ของกิจกรรมหลัก (core activities) ที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ และมี
ข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
(มาตรา 41 (2))

กรณีที่สาม หากกิจกรรมหลักกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วน
บุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลประเภทอ่อนไหว (มาตรา 26) ก็ต้องจัดให้มี
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย (มาตรา 41 (3))

2.6 หลักการในการประมวลผลข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือที่เรียกรวมกันว่าการประมวลผลข้อมูลส่วนบุคคลนั้น มีหลักการ 7 ประการ ดังภาพนี้



หลักการประมวลผลข้อมูลส่วนบุคคล

- 1) หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness Fairness and Transparency) ซึ่งหมายถึงการประมวลผลข้อมูลส่วนบุคคล จะต้องมียุทธศาสตร์ดังนี้
 - การประมวลผลโดยชอบด้วยกฎหมาย (Lawfulness) หมายถึง ประมวลผลตามฐานในการประมวลผล
 - การประมวลผลที่เป็นธรรม (Fairness) หมายถึง การประมวลผลนั้นจะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล และจะต้องไม่ก่อให้เกิดผลกระทบทางด้านลบต่อเจ้าของข้อมูล
 - การประมวลผลต้องมีความโปร่งใส (Transparency) หมายถึง การประมวลผลนั้นนอกจากจะต้องชอบด้วยกฎหมายและเป็นธรรม จะต้องมีความโปร่งใสกล่าวคือสามารถตรวจสอบได้ว่าใช้หลักในการประมวลผลตรงตามหลักของการประมวลผลข้อมูลส่วนบุคคล
- 2) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) การประมวลผลข้อมูลสามารถกระทำได้อย่างจำกัดเท่าที่จำเป็นภายใต้ขอบเขตวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล เพื่อให้การประมวลผลข้อมูลส่วนบุคคลสอดคล้องตามและชอบด้วยกฎหมาย
- 3) หลักการใช้ข้อมูลอย่างจำกัด (Data Minimization) การประมวลผลจะต้องมีการเก็บข้อมูลตามเท่าที่จำเป็น และควรพิจารณาถึงความจำเป็นในการเก็บรวบรวมข้อมูล ตัวอย่างเช่น การเก็บเก็บสำเนาบัตรประชาชน ซึ่งมีข้อมูลศาสนาซึ่งเป็นข้อมูลอ่อนไหวตามมาตรา 26 โรงแรมต้องพิจารณาว่าการเก็บข้อมูลศาสนาดังกล่าว มีความจำเป็นต้องเก็บหรือไม่ เพราะถ้าหากไม่

มีความจำเป็นในการเก็บแล้ว ควรมีมาตรการบางอย่าง เช่น การถมดำ หรือ การขีดฆ่าข้อมูล ศาสนาในสำเนา เพื่อเป็นการลดภาระและปัญหาที่ตามมาจากการเก็บข้อมูลอ่อนไหว

- 4) หลักความถูกต้องของข้อมูล (Accuracy) ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันและจะต้องดำเนินการเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบ หรือ แก้ไขโดยไม่ชักช้า
- 5) หลักการการจัดเก็บข้อมูลอย่างจำกัด (Storage Limitation) ข้อมูลส่วนบุคคลจะต้องเก็บใน ระยะเวลาที่เหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ในการประมวลผลข้อมูล รวมถึงมี กระบวนการดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บ รักษา
- 6) หลักการดำรงไว้ซึ่งความถูกต้องสมบูรณ์ และความลับของข้อมูล (Integrity and Confidentiality) มาตรการที่จะรักษาความปลอดภัยให้ข้อมูลส่วนบุคคลนั้นจะต้องมีความ สมบูรณ์ และเป็นความลับ โดยต้องไม่มีใครเข้าถึงข้อมูลหากไม่มีสิทธิ
- 7) หลักความรับผิดชอบของผู้ควบคุมข้อมูล (Accountability) หมายถึงว่าการประมวลผล ข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลความรับผิดชอบรวมถึงดำเนินการให้สอดคล้อง ตามหลักของการคุ้มครองข้อมูลส่วนบุคคล

2.7 ฐานทางกฎหมาย (Lawful Basis)

ตามหลักของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อมีการเก็บรวบรวมข้อมูล ส่วน บุคคล จำเป็นจะต้องขอความยินยอมก่อน (ซึ่งปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 19) เว้นแต่เข้าข้อยกเว้นตามมาตรา 24 หรือ 26 ซึ่งฐานทางกฎหมายจะมี 2 กลุ่มหลัก ๆ ได้แก่ ฐานการประมวลผล ข้อมูลส่วนบุคคลทั่วไปและฐานการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยแต่ละประเภทมี รายละเอียดดังต่อไปนี้

ฐานการประมวลผลข้อมูลส่วนบุคคลทั่วไป ตามมาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูล ส่วน บุคคล พ.ศ. 2562 มีดังต่อไปนี้

1. ฐานความยินยอม (Consent) จากที่กล่าวในข้างต้นไปแล้ว การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล จำเป็นต้องมีการขอความยินยอมก่อน เว้นแต่จะมีข้อยกเว้นตามกฎหมาย ซึ่งถ้ากิจกรรม ดังกล่าวไม่มีฐานในการรองรับตามกฎหมายจำเป็นต้องมีการขอความยินยอม โดยการขอความยินยอมจะมี หลักเกณฑ์ดังนี้

- 1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอ “ก่อนหรือในขณะที่” ประมวลผลข้อมูล ส่วน บุคคล
- 2) การขอความยินยอมต้องทำโดยชัดแจ้ง แยกส่วนจากข้อความอื่นอย่างชัดเจน
- 3) แจ้งวัตถุประสงค์อย่างชัดเจน

- 4) ใช้ข้อความที่เข้าถึงได้ง่าย และเข้าใจได้
- 5) ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงทำให้เข้าใจผิดในวัตถุประสงค์
- 6) การให้ความยินยอมต้องมีความอิสระ และต้องไม่เป็นส่วนหนึ่งของสัญญา หรือบริการ
- 7) ต้องถอดถอนง่ายเช่นเดียวกับตอนให้ความยินยอม และจะถอนความยินยอมเมื่อใดก็ได้
- 8) หากการถอนความยินยอมมีผลกระทบในเรื่องใด ต้องแจ้งให้เจ้าของข้อมูลทราบ

ก่อนที่กฎหมายจะบังคับใช้ โรงแรมย่อมมีการเก็บข้อมูลส่วนบุคคลไว้อยู่ก่อนแล้ว เช่น ประวัติการเข้าพักของนักท่องเที่ยว หรือบริการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้ประกอบการอาจเกิดคำถามว่า ข้อมูลที่เก็บมาก่อนหน้ากฎหมายบังคับใช้จะทำการอย่างไรเพื่อให้เป็นไปตามกฎหมาย ซึ่งคำตอบนั้นกฎหมายได้มีการระบุไว้โดยสังเขป คือ ข้อมูลส่วนบุคคลที่มีการเก็บก่อนหน้าที่กฎหมายบังคับใช้ก็สามารถใช้ได้ตามปกติหรือตามวัตถุประสงค์เดิม แต่ต้องมีช่องทางให้เจ้าของข้อมูลสามารถถอนความยินยอม เป็นไปตามบทเฉพาะกาล มาตรา 95

กรณีที่นักท่องเที่ยว เป็นบุคคลหย่อนความสามารถ อันได้แก่ ผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมาย คนเสมือนไร้ความสามารถ และคนไร้ความสามารถ การขอความยินยอมกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหลักเกณฑ์ในการขอความยินยอมเพิ่มเติม ปรากฏตามมาตรา 20 ดังนี้

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

(1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง

(2) ผู้เยาว์อายุ 10 ปี แต่ยังไม่ถึง 20 ปีบริบูรณ์ อาจให้ความยินยอมโดยลำพัง หรือจาก ผู้ใช้อำนาจปกครองผู้เยาว์

(3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์

(4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

รวมถึงการถอนความยินยอม การแจ้งให้ทราบ การใช้สิทธิ การร้องเรียน และอื่น ๆ ตามพระราชบัญญัติ ให้กระทำโดยผู้มีอำนาจตาม (1) - (4) ด้วย

2 ฐานปฏิบัติตามสัญญา (Contract) ฐานสัญญาถือเป็นฐานที่จำเป็นเพื่อการปฏิบัติตามสัญญาและใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะเข้าทำสัญญา เช่น การจองห้องพัก โรงแรม การเก็บข้อมูลพื้นฐานเพื่อการเข้าพัก เป็นต้น โดยแม้ไม่ได้ระบุเป็นเงื่อนไขในสัญญา

มีข้อสังเกตว่าฐานปฏิบัติตามสัญญา จะครอบคลุมถึงข้อมูลส่วนบุคคลประเภททั่วไปเท่านั้น จะไม่รวมถึงข้อมูลส่วนบุคคลประเภทอ่อนไหว

3 ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation) ฐานการปฏิบัติหน้าที่ตามกฎหมายของโรงแรม ซึ่งเป็นกรณีที่มีกฎหมายกำหนดหน้าที่ให้โรงแรมต้องดำเนินการเก็บรวบรวม ใช้ เผยแพร่ข้อมูลส่วนบุคคลอยู่แล้ว เช่น กิจกรรมการกรอกใบ รร.3 หรือ แบบ ตม.30

4 ฐานผลประโยชน์สาธารณะ อำนาจอรัฐ (Public Task) ผู้ประมวลผลข้อมูลตามฐานนี้มักเป็นเจ้าหน้าที่ หรือหน่วยงานของรัฐที่มีหน้าที่ในการปฏิบัติตามภารกิจที่มีกฎหมายกำหนดไว้ รวมถึงหน่วยงานเอกชน หากการประมวลผลข้อมูลนั้นมีความจำเป็นหรือหน้าที่ที่ต้องปฏิบัติตามกฎหมายหรือเป็นไปเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย

5 ฐานผลประโยชน์อันชอบธรรมด้วยกฎหมาย (Legitimate Interest) โรงแรมจะใช้ฐานนี้ในกรณีที่ต้องดำเนินการดำเนินการเพื่อประโยชน์อันชอบธรรมของโรงแรม และเป็นไปอย่างสมเหตุสมผล เช่น กิจกรรมการบันทึกภาพเคลื่อนไหวด้วยกล้องวงจรปิด (CCTV) เพื่อวัตถุประสงค์ในการปกป้องพื้นที่ทรัพย์สิน และป้องกันอาชญากรรมและการลักทรัพย์ ทุจริตฉ้อโกง เป็นต้น หากโรงแรมจะใช้ฐานนี้ควรประเมินความจำเป็นภายใต้ 3 องค์ประกอบดังต่อไปนี้

- 1) จะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล
- 2) มีความเสี่ยงต่อการกระทบสิทธิเสรีภาพของเจ้าของข้อมูลในระดับต่ำ
- 3) มีความชอบธรรม

6 ฐานระงับอันตรายต่อ ร่างกาย สุขภาพ หรือชีวิต (Vital Interest) ฐานระงับอันตรายต่อร่างกาย สุขภาพ หรือชีวิต หากกรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อน (Sensitive Data) เช่น หมู่อเล็ด ข้อมูลสุขภาพ สามารถใช้ได้กรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เช่น เจ้าของข้อมูลส่วนบุคคลเกิดอุบัติเหตุ แต่หากขอความยินยอมได้ควรขอก่อน ตามมาตรา 24 เป็น ข้อมูลทั่วไป และมาตรา 26 เป็นข้อมูลอ่อนไหวกรณีไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใด

7 ฐานการจัดทำเอกสารประวัติศาสตร์-วิจัย-สถิติ และจดหมายเหตุ (Historical Document, Research, or Statistics) ในฐานจดหมายเหตุ วิจัย สถิติ นี้ไม่มีใน GDPR แต่อย่างไรก็ตามควรเป็นไปตามมาตรฐานการวิจัย เป็นการเก็บรวบรวม จัดเก็บข้อมูลเพื่อการจัดทำเอกสารทางประวัติศาสตร์ หรืองานวิจัย หรืองานสถิติ ซึ่งจะต้องมีการระบุชัดเจน

ฐานการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว ตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีดังต่อไปนี้

1. ฐานความยินยอม (Consent) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว จำเป็นต้องมีการขอความยินยอมก่อน เว้นแต่จะมีข้อยกเว้นตามกฎหมาย ซึ่งถ้ากิจกรรมดังกล่าวไม่มีฐานในการรองรับตามกฎหมายจำเป็นต้องมีการขอความยินยอม โดยการขอความยินยอมจะมีหลักเกณฑ์ดังนี้

- 1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอ “ก่อนหรือในขณะที่” ประมวลผลข้อมูลส่วนบุคคล
- 2) การขอความยินยอมต้องทำโดยชัดแจ้ง แยกส่วนจากข้อความอื่นอย่างชัดเจน
- 3) แจ้งวัตถุประสงค์อย่างชัดเจน
- 4) ใช้ข้อความที่เข้าใจได้ง่าย และเข้าใจได้
- 5) ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงทำให้เข้าใจผิดในวัตถุประสงค์

- 6) การให้ความยินยอมต้องมีความอิสระ และต้องไม่เป็นส่วนหนึ่งของสัญญา หรือบริการ
- 7) ต้องถอดถอนง่ายเช่นเดียวกับตอนให้ความยินยอม และจะถอนความยินยอมเมื่อใดก็ได้
- 8) หากการถอนความยินยอมมีผลกระทบในเรื่องใด ต้องแจ้งให้เจ้าของข้อมูลทราบ

ก่อนที่กฎหมายจะบังคับใช้ โรงแรมย่อมมีการเก็บข้อมูลส่วนบุคคลอ่อนไหวไว้อยู่ก่อนแล้ว เช่น ข้อมูลการแพ้อาหาร ข้อมูลความพิการ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้ประกอบการอาจเกิดคำถามว่า ข้อมูลที่เก็บมาก่อนหน้ากฎหมายบังคับใช้จะอย่างไรเพื่อให้เป็นไปตามกฎหมาย ซึ่งคำตอบนั้นกฎหมายได้มีการระบุไว้โดยสังเขป คือ ข้อมูลส่วนบุคคลที่มีการเก็บก่อนหน้าที่ยกกฎหมายบังคับใช้ก็สามารถใช้ได้ตามปกติหรือตามวัตถุประสงค์เดิม แต่ต้องมีช่องทางให้เจ้าของข้อมูลสามารถถอนความยินยอม เป็นไปตามบทเฉพาะกาล มาตรา 95

กรณีที่นักท่องเที่ยว เป็นบุคคลหย่อนความสามารถ อันได้แก่ ผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมาย คนเสมือนไร้ความสามารถ และคนไร้ความสามารถ การขอความยินยอมกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหลักเกณฑ์ในการขอความยินยอมเพิ่มเติม ปรากฏตามมาตรา 20 ดังนี้

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

- (1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง
- (2) ผู้เยาว์อายุ 10 ปี แต่ยังไม่ถึง 20 ปีบริบูรณ์ อาจให้ความยินยอมโดยลำพัง หรือจาก ผู้ใช้อำนาจปกครองผู้เยาว์
- (3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์
- (4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

รวมถึงการถอนความยินยอม การแจ้งให้ทราบ การใช้สิทธิ การร้องเรียน และอื่น ๆ ตามพระราชบัญญัติ ให้กระทำโดยผู้มีอำนาจตาม (1) - (4) ด้วย

2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ในกรณีที่นักท่องเที่ยวไม่สามารถให้ความยินยอมได้ ฐานระงับอันตรายต่อร่างกายสุขภาพและชีวิตกรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อน (Sensitive Data) เช่น กรู๊ปเลือด ข้อมูลสุขภาพ สามารถใช้ได้กรณีที่แขกไม่สามารถให้ความยินยอมได้ เช่น นักท่องเที่ยวหรือพนักงานเองเกิดอุบัติเหตุ แล้วอยู่ในสภาพหมดสติ เป็นต้น

3. เป็นการดำเนินการกิจกรรมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ประชญา หรือ สหภาพแรงงานให้แก่สมาชิก เช่น มูลนิธิแผ่นดินธรรม วัด โบสถ์ พรรคการเมือง สหภาพแรงงานรัฐวิสาหกิจ ข้อยกเว้นนี้กำหนดเฉพาะกิจกรรมที่ใช้เป็นการเฉพาะเท่านั้น ตัวอย่างเช่น วัดมีการรวบรวมข้อมูลการนับถือศาสนาในบริเวณโดยรอบวัดเพื่อจะจัดส่งซองผ้าป่า เป็นต้น ทั้งนี้จะต้องใช้เป็นการส่วนตัวของมูลนิธิ หรือองค์กรเองโดยไม่เปิดเผยไปสู่บุคคลภายนอก

4. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น การแต่งกายที่บ่งบอกถึงการนับถือศาสนาในที่สาธารณะ หรือการประกาศผ่านช่องทางสื่อสังคมต่าง ๆ

5. จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย เช่น การเก็บลายนิ้วมือของผู้เสียหายเพื่อเป็นหลักฐานในการเอาผิดผู้กระทำความผิด เป็นต้น

6. จำเป็นต้องปฏิบัติตามกฎหมาย เฉพาะที่เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์การประเมินความสามารถในการทำงานของเจ้าของข้อมูลส่วนบุคคล การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ประโยชน์สาธารณะด้านสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นที่สำคัญ

2.8 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ “ไม่ใช่” จากเจ้าของข้อมูลโดยตรง

ในบางครั้งทางผู้ประกอบการโรงแรมอาจจำเป็นต้องเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจากแหล่งอื่น เช่น เก็บข้อมูลผู้ที่สามารถติดต่อได้เพื่อการสมัครงาน ตามหลักของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 ได้วางแนวทางพอสังเขปว่า ไม่สามารถเก็บข้อมูลส่วนบุคคลการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลได้ เว้นแต่กรณีดังต่อไปนี้

1. ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่แขก หรือ ลูกจ้าง หรือ คู่ค้าทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากนักท่องเที่ยว ลูกจ้าง หรือคู่ค้า

2. เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีฐานทางกฎหมาย (Lawful Basis)

ทั้งนี้ ทางโรงแรมต้องแจ้งรายละเอียดวัตถุประสงค์ใหม่ในการเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 เว้นแต่กรณีดังต่อไปนี้

- 1) นักท่องเที่ยว ลูกจ้าง หรือคู่ค้าทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว
- 2) โรงแรมพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- 3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของ เจ้าของข้อมูลส่วนบุคคล ซึ่งได้แก่นักท่องเที่ยว ลูกจ้าง หรือ คู่ค้า
- 4) เมื่อโรงแรมเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามมาตรา 25 ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 30 วันนับแต่วันที่เก็บรวบรวมข้อมูลส่วนบุคคลนั้น เว้นแต่กรณีที่น่าข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

2.9 การใช้ หรือการเปิดเผยข้อมูล

โดยหลักทั่วไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การนำข้อมูลส่วนบุคคลมาใช้ หรือเปิดเผย จำเป็นจะต้องได้รับความยินยอมก่อนเสมอ เว้นแต่เป็นการเก็บรวบรวมตามฐานทางกฎหมาย แม้ว่าจะมีฐานทางกฎหมายสามารถให้ผู้ประกอบการมีสิทธิใช้ข้อมูลส่วนบุคคลก็ตาม แต่ผู้ประกอบการในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องคิดไว้เสมอว่าการใช้ข้อมูลส่วนบุคคลจำเป็นที่จะต้องคำนึงถึงหลักของการใช้ข้อมูลส่วนบุคคลตามหลักหลักการจำกัดวัตถุประสงค์ (Purpose Limitation)

2.10 การส่งหรือโอนข้อมูลไปต่างประเทศ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้กำหนดกรณีการส่งต่อหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศนั้นสามารถทำได้ ซึ่งหลักการโอนข้อมูลส่วนบุคคลจำเป็นต้องมาตามฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่เข้าข้อยกเว้นดังต่อไปนี้

- 1) เป็นการปฏิบัติตามกฎหมาย
- 2) ได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งต้องมีการแจ้งให้ทราบถึงมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลประเทศปลายทาง
- 3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- 4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- 5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- 6) เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ

2.11 สิทธิของเจ้าของข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดสิทธิ 9 สิทธิ ได้แก่

- 1) สิทธิในการได้รับแจ้ง (Right to be Informed) มาตรา 23 เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการที่จะได้ทราบถึงรายละเอียดเกี่ยวกับการใช้ข้อมูลของผู้ควบคุมข้อมูลหรือเหตุการณ์ต่าง ๆ โดยต้องทำการแจ้งก่อน หรือขณะที่มีการประมวลผลข้อมูลส่วนบุคคล เพื่อเจ้าของข้อมูลส่วนบุคคล

บุคคลสามารถตัดสินใจเกี่ยวกับข้อมูลอันอาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้ ซึ่งสิ่งที่ผู้ประกอบการแจ้งให้เจ้าของข้อมูลทราบได้แก่

- วัตถุประสงค์ในการเก็บรวบรวมข้อมูล
- เก็บข้อมูลอะไรบ้าง รวมถึงเป็นระยะเวลานานเท่าใด
- ส่งต่อหรือเปิดเผยให้หน่วยงานใด
- ช่องทางติดต่อเพื่อใช้สิทธิของเจ้าของข้อมูล
- เจ้าของข้อมูลมีสิทธิอะไรบ้าง

2) สิทธิในการถอนความยินยอม (Right to Withdraw Consent) มาตรา 19 วรรคห้า เป็นสิทธิที่เจ้าของข้อมูลสามารถถอนความยินยอมที่ได้เคยให้ไว้กับผู้ประกอบการ ซึ่งหลักของการถอนความยินยอมมีดังนี้

- การถอนความยินยอมจะต้องถอนเมื่อใดก็ได้
- ต้องถอนได้โดยวิธีที่ง่ายเหมือนเมื่อตอนให้คำยินยอม
- การถอนต้องไม่มีผลย้อนหลังและไม่ส่งผลต่อการประมวลผลที่ยินยอมไปก่อนหน้านี้
- ต้องแจ้งถึงผลกระทบในการถอนความยินยอม

3) สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right to be Access) หมายถึง เจ้าของข้อมูลมีสิทธิที่เข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวข้องกับตนหรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ไม่ได้ให้ความยินยอม โดยเจ้าของข้อมูลส่วนบุคคลจะต้องดำเนินการให้เสร็จภายใน 30 วัน นับแต่ได้รับคำร้อง

4) สิทธิในการโอนย้ายข้อมูล (Right to Data Portability) หมายถึง เจ้าของข้อมูลให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการดังต่อไปนี้

- โอนข้อมูลไปยังผู้ควบคุมอื่น
- ขอรับข้อมูลจากผู้ควบคุมข้อมูล ส่ง หรือโอน ไปผู้ควบคุมข้อมูลอื่นโดยตรง แต่มีข้อยกเว้นว่าไม่สามารถทำได้โดยสภาพ

สิทธิการโอนย้ายข้อมูลตามสิทธิดังกล่าวมีหลักสำคัญได้แก่ เป็นไปเพื่อความจำเป็นของของผู้ควบคุม และคำขอจะต้องไม่กระทบต่อสิทธิของบุคคลอื่น

5) สิทธิคัดค้านการใช้ข้อมูล (Right to Object) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในกรณีที่ผู้ประกอบการในฐานะผู้ควบคุมข้อมูลส่วนบุคคล นำข้อมูลส่วนบุคคลไปใช้ไม่เป็นไปตามวัตถุประสงค์ ยกตัวอย่างเช่น นำข้อมูลส่วนบุคคลของนักท่องเที่ยวไปใช้เพื่อเสนอบริการอื่นที่ไม่เกี่ยวกับธุรกิจท่องเที่ยว เช่น การนำข้อมูลไปขายเพื่อผลประโยชน์อื่น เป็นต้น

สิทธิในการคัดค้านยังรวมถึง การที่ผู้ประกอบการนำข้อมูลไปใช้โดยไม่ขอความยินยอมด้วย กล่าวคือ แม้ว่าการกิจกรรมจะมีการดำเนินการเนื่องจากเกี่ยวข้องกับธุรกิจโรงแรมก็

ตาม แต่ไม่มีการขอความยินยอมก่อนผู้ที่เป็นเจ้าของข้อมูลก็สามารถที่จะทำการคัดค้านได้ ตัวอย่างที่เห็นภาพได้แก่ การทำการตลาดโดยตรงหรือที่เรียกว่า Direct Marketing ซึ่งแม้จะเป็นกิจกรรมการส่งเสริมการขายให้แก่ธุรกิจโรงแรม แต่กิจกรรมการทำธุรกิจโดยตรงจำเป็นต้องมีการขอความยินยอมก่อน ซึ่งถ้านักท่องเที่ยวไม่ได้ให้ความยินยอม ก็ไม่สามารถทำได้

- 6) สิทธิขอให้ลบข้อมูล ทำลาย ทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (Right to be Forgotten) หมายถึง เจ้าของข้อมูลมีสิทธิขอให้ลบ ทำลาย หรือ ทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีดังต่อไปนี้

- กรณีที่หมดความจำเป็นในการเก็บข้อมูล เช่น เมื่อถึงกำหนดระยะเวลาการเก็บรักษา หรือเมื่อไม่มีความจำเป็นต้องใช้งาน
- เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม และผู้ควบคุมข้อมูลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผย แต่หากว่าผู้ประกอบการสามารถพิสูจน์ได้ว่า ยังมีความจำเป็นต้องใช้งานต่อ เช่น จำต้องเก็บไว้จนครบกำหนดสัญญา หรือ ยังไม่ถึงกำหนดระยะเวลาในการลบหรือทำลายข้อมูล เจ้าของข้อมูลสามารถปฏิเสธคำขอได้ โดยผู้ประกอบการจะต้องมีการแสดงเหตุผลในการปฏิเสธไว้ด้วย
- เมื่อเจ้าของข้อมูลคัดค้าน ตามข้อ 5)
- เมื่อเป็นการได้ข้อมูลมาโดยไม่ถูกต้องตามกฎหมาย เช่น ได้มาโดยไม่ได้รับความยินยอม กรณีดังกล่าว หากเจ้าของข้อมูลมาใช้สิทธิผู้ประกอบการก็ต้องดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล

- 7) สิทธิขอให้ระงับใช้ข้อมูล (Right to Restrict Processing) ตามมาตรา 34 เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิขอให้ระงับ ซึ่งการระงับตามสิทธิดังกล่าวหมายถึง การขอให้ผู้ประกอบการงดหรือห้ามใช้ข้อมูลของเจ้าของข้อมูล เป็นการชั่วคราว ไปจนกว่าเจ้าของข้อมูลจะอนุญาตให้ดำเนินการต่อไปได้ เช่น ประมวลผลต่อ หรือลบ ทำลายไป โดยสิทธิการระงับการใช้ข้อมูล สามารถใช้ในกรณีดังต่อไปนี้

- กรณีอยู่ในระหว่างการพิจารณาแก้ไข ลบ หรือทำลายข้อมูล กรณีนี้เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิให้แก้ไข ลบ หรือทำลายข้อมูล ในระหว่างที่โรงแรมกำลังพิจารณาการใช้สิทธิ โรงแรมสามารถระงับการประมวลผลข้อมูลไปก่อนจนกว่าจะพิจารณาการใช้สิทธิเสร็จสิ้น
- กรณีเมื่อถึงกำหนดระยะเวลาการทำลาย แต่เจ้าของข้อมูลขอใช้สิทธิขอให้ระงับข้อมูล ยกตัวอย่างเช่น เจ้าของข้อมูล จำเป็นต้องใช้ข้อมูลจากผู้ประกอบการเพื่อการพิจารณาคดี ดังนั้นจึงขอให้ทางผู้ประกอบการระงับการทำลายข้อมูลก่อน

- 8) สิทธิในการแก้ไขข้อมูล (Right to Rectification) เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการแก้ไขข้อมูลให้ถูกต้อง โดยปกติผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการประมวลผลข้อมูลที่ทันสมัยและถูกต้องอยู่เสมอ ทั้งนี้ ในบางกรณีอาจไม่สามารถรับรู้หรือทราบถึงข้อมูล ที่ถูกต้องในกรณีนี้เจ้าของข้อมูลส่วนบุคคลสามารถยื่นคำขอใช้สิทธิแก้ไขข้อมูลให้ถูกต้อง รวมไปถึงขอเพิ่มเติมหรือลบข้อมูลเพื่อทำข้อมูลให้เป็นปัจจุบัน
- 9) สิทธิในการร้องเรียน เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องเรียน ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล รวมถึง ลูกจ้าง ผู้รับจ้าง ของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ที่ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

2.12 บทกำหนดโทษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการพูดถึงบทลงโทษของผู้ประกอบการที่ไม่ยอมปฏิบัติตาม โดยโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีดังนี้

1. ความรับผิดทางแพ่ง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดความรับผิดทางแพ่งไว้ โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล จะต้องชดเชยค่าสินไหม

มีข้อสังเกตว่า ค่าสินไหมครอบคลุมไปถึงไหน โดยพระราชบัญญัติได้มีการระบุไว้ชัดเจนว่ารวมไปถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นแล้ว ดังนั้นค่าเสียหายที่สามารถฟ้องได้จึงรวมไปถึงค่าเสียหายที่เกิดจากการปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูลด้วย ทั้งนี้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทน แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น

2. ความรับผิดอาญา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดบทกำหนดโทษในส่วน of โทษอาญาไว้ในกรณีต่าง ๆ ดังต่อไปนี้

- 1) ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) โดยมีขอบหรือนอกเหนือวัตถุประสงค์ หรือส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) ไปยังต่างประเทศ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- 2) ผู้ใดซึ่งล่วงรู้ข้อมูลส่วนบุคคลเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้แล้วนำไปเปิดเผยแก่ผู้อื่น โดยมีขอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

โดยมีข้อยกเว้น สำหรับบทลงโทษนี้ มิให้นำมาบังคับใช้แก่การเปิดเผย ในกรณีดังนี้

- เปิดเผยตามหน้าที่
- เปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือพิจารณาคดี
- เปิดเผยแก่หน่วยงานรัฐในประเทศ หรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- การเปิดเผยเกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

3) กรรมการหรือผู้จัดการหรือบุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคล หากมีการสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจำเป็นเหตุให้นิติบุคคลกระทำความผิดต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย

3. ความรับผิดทางปกครอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติบทกำหนดโทษ ส่วนของโทษทางปกครองในหมวดที่ 7 ซึ่งมีโทษปรับสูงสุดไม่เกิน 5,000,000 บาท ความรับผิดทางปกครองคณะกรรมการผู้เชี่ยวชาญจะเป็นผู้พิจารณา โดยหลักพิจารณาได้แก่

- ความร้ายแรงแห่งพฤติกรรมที่กระทำ
- ขนาดกิจการของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล
- พฤติการณ์

3. กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับธุรกิจโรงแรมและที่พัก

3.1 ภาพรวมธุรกิจโรงแรมและที่พัก

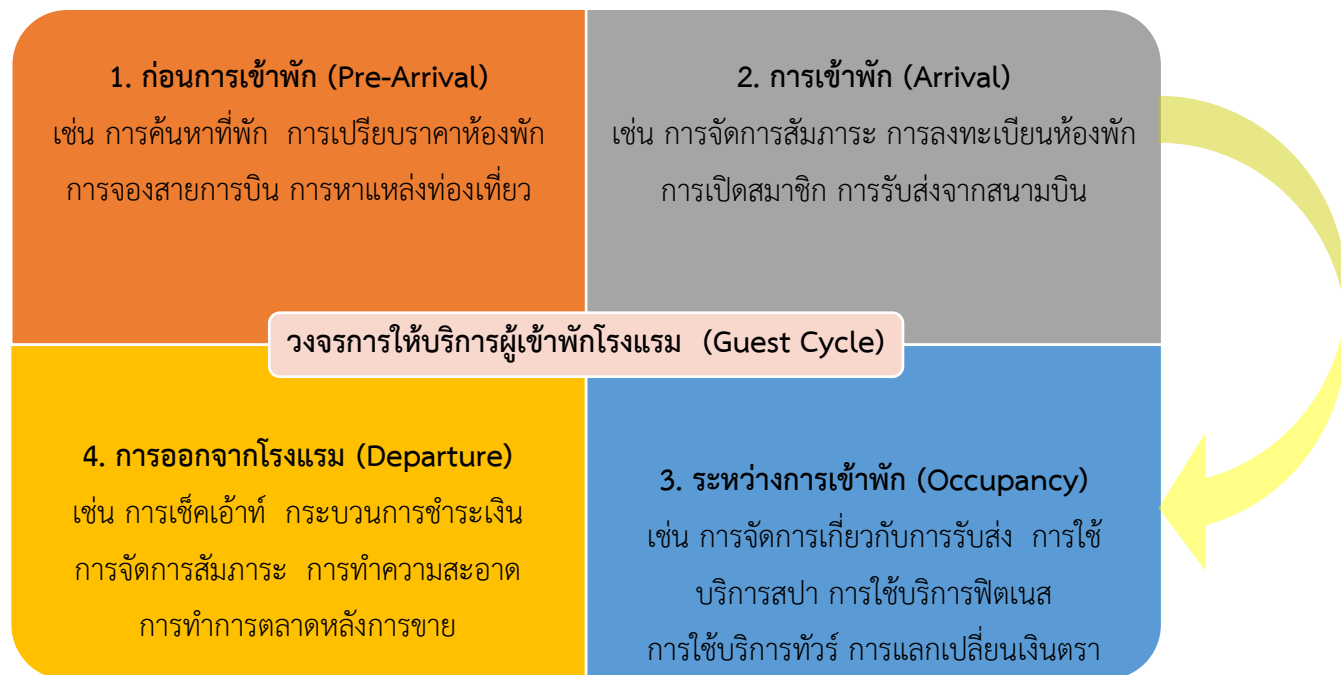
ในปัจจุบัน อุตสาหกรรมการท่องเที่ยวหลังสถานการณ์โควิด มีการคาดการณ์ว่าจะโตขึ้นมากกว่า 20% ตามการคาดการณ์ของการท่องเที่ยวแห่งประเทศไทย (ททท.) ซึ่งเมื่อสถานการณ์ด้านการท่องเที่ยวของประเทศไทยดีขึ้นย่อมส่งผลให้จำนวนคนที่เข้ามาท่องเที่ยวก็จะมีมากขึ้นตามมา ไม่ว่าจะเป็นนักท่องเที่ยวที่เป็นคนในประเทศเอง และนักท่องเที่ยวจากต่างประเทศ

อีกทั้งเมื่อไม่นานมานี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีการบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 รวมถึงกฎหมายฉบับรองที่ทยอยออกมานั้น ทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เข้าไปมีบทบาทกับอุตสาหกรรมการท่องเที่ยวอย่างสูง เนื่องจากกระบวนการในอุตสาหกรรมมีการเก็บข้อมูลของบุคคลจำนวนมาก ไม่ว่าจะเป็นข้อมูลที่ได้มาจากการลงทะเบียน หรือการจองที่พัก การจองทัวร์ การจัดนิทรรศการ เป็นต้น

แม้ว่าอุตสาหกรรมการท่องเที่ยวประกอบไปด้วยธุรกิจมากมาย ตั้งแต่ ธุรกิจนำเที่ยวและมัคคุเทศก์ ธุรกิจโรงแรมและที่พัก ธุรกิจร้านขายของที่ระลึก ธุรกิจขนส่ง ธุรกิจสปา ไปจนถึงภัตตาคาร ธุรกิจสถานบันเทิง แต่เนื่องด้วยข้อจำกัดด้านทรัพยากร แนวปฏิบัติฉบับนี้จึงจะกล่าวถึงเฉพาะเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับธุรกิจ “โรงแรมและที่พัก” และในขอบเขตของ “แขก” ผู้เข้าพักในฐานะเจ้าของข้อมูลส่วนบุคคลเท่านั้น

การคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นเรื่องสำคัญที่ผู้ประกอบการโรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องให้ความสำคัญ เพราะไม่เพียงส่งผลต่อความน่าเชื่อถือในชื่อเสียง (Goodwill) ของโรงแรมแต่ยังส่งผลต่อความไว้วางใจ (Trust & Confidence) ของแขกที่ให้การบริการของโรงแรม การปฏิบัติให้เป็นไปตามกฎหมาย (Compliance) จึงมีความจำเป็นที่จะต้องใช้ทรัพยากรทั้งด้านบุคลากรและเวลาในการปรับตัวให้สอดคล้องกับกฎหมาย ดังกล่าว ดังนั้นผู้บริหารควรมีการกำหนดนโยบาย มอบหมายผู้รับผิดชอบในการผลักดันแผนงาน พร้อมทั้งสนับสนุนงบประมาณเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นเครื่องมือทางธุรกิจที่สามารถทำงานประสานกันจนเป็นส่วนหนึ่งของแผนกลยุทธ์ขององค์กร เพื่อให้บรรลุเป้าหมายทางธุรกิจได้ในที่สุด

3.2 วงจรการให้บริการผู้เข้าพักโรงแรม (Guest Cycle) และ วงจรชีวิตข้อมูลส่วนบุคคล (Data Life Cycle)

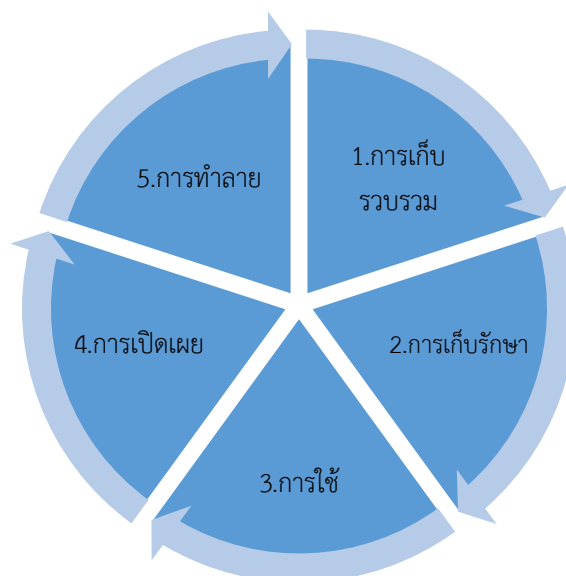


ภาพแสดงวงจรการให้บริการผู้เข้าพักที่เข้าพักโรงแรม (Guest Cycle)

ในธุรกิจโรงแรมและที่พักนั้น โดยหลักแล้วกิจกรรมที่เกิดขึ้นทั้งวงจรนั้น สามารถพิจารณาได้จาก “วงจรการให้บริการผู้เข้าพักโรงแรม (Guest Cycle)” ซึ่งก็คือ วิธีการและขั้นตอนตั้งแต่เริ่มต้นของผู้เข้าพัก ตั้งแต่การค้นหาโรงแรม จนถึงการเข้าพักและจากไป และจะกลับมาพักใหม่ ซึ่งโดยหลักแล้วประกอบด้วย 4 ขั้นตอนดังต่อไปนี้

- 1) ก่อนการเข้าพัก (Pre-Arrival)** เป็นขั้นตอนที่เริ่มตั้งแต่จองห้องพักทางช่องทางต่าง ๆ จนถึงก่อนที่นักท่องเที่ยวเช็คอินเข้าพัก ซึ่งรวมไปถึงการบริการก่อนถึงที่พัก ก่อนการเข้าพัก ผู้เข้าพักยังเดินทางมาไม่ถึงโรงแรม แต่ผู้เข้าพักอาจต้องการบริการต่าง ๆ จากโรงแรม เช่น บริการรับส่ง ที่สนามบิน เป็นต้น
- 2) การเข้าพัก (Arrival)** เป็นขั้นตอนการเข้าพักเมื่อผู้เข้าพักมาถึงโรงแรม กิจกรรมหลัก ๆ ประกอบด้วย การลงทะเบียนเข้าพัก (Registration) การลงทะเบียนเข้าพักทั้งนักท่องเที่ยวในประเทศและต่างประเทศตามกฎหมาย จนกระทั่งนักท่องเที่ยวเข้าพักในโรงแรม
- 3) ระหว่างการเข้าพัก (Occupancy)** เป็นขั้นตอนหลังจากการส่งผู้เข้าพักเข้าห้องพัก ซึ่งแผนกต้อนรับส่วนหน้ายังคงทำหน้าที่ในการประสานงาน ให้บริการต่าง ๆ และการจัดเตรียมข้อมูลเพื่อการบริการ ในระหว่างที่นักท่องเที่ยวเข้าพักในโรงแรม

- 4) การออกจากโรงแรม (Departure) จะเป็นขั้นตอนตั้งแต่ออกจากห้องพัก ชำระค่าบริการ บันทึกประวัติข้อมูลผู้เข้าพักจนกระทั่งถึงการไปส่งที่จุดหมาย อาจจะเป็นสนามบิน และรวมไปถึงการทำตลาดหลังการขาย ซึ่งเป็นขั้นตอนสุดท้ายในวงจรผู้เข้าพัก



ภาพแสดงวงจรชีวิตข้อมูลส่วนบุคคล (Data life cycle)

ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น เราพิจารณาเฉพาะกิจกรรมที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเท่านั้น ดังนั้นเมื่อพิจารณากิจกรรมจาก “วงจรการให้บริการผู้เข้าพักที่เข้าพักโรงแรม (Guest Cycle)” ข้างต้นแล้ว ตั้งแต่ การเก็บ เก็บรักษา ใช้ เปิดเผย และ ทำลายข้อมูล เราจึงจะสามารถระบุกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้ดังนี้

- 1) กระบวนการลูกค้าค้นหาที่พัก เปรียบเทียบราคา จนกระทั่งนักท่องเที่ยวสนใจและตัดสินใจจองห้องพัก ซึ่งก็เป็นไปได้ทั้งการจองห้องพักตรงกับโรงแรม ไม่ว่าจะทางเว็บไซต์ โทรศัพท์ อีเมล หรือแพลตฟอร์มการสื่อสารอื่น ๆ เช่น Line OA หรือ Facebook Messenger หรืออาจจะตัดสินใจไปจองผ่าน OTA หรือการ Walk-in ก็เป็นไปได้
- 2) กระบวนการการเข้าพัก ซึ่งจะผ่านขั้นตอนการเช็คอิน ลูกค้ากรอกแบบฟอร์มต่าง ๆ โดยเฉพาะ Registration Form ที่โรงแรมต้องส่งรายงานและเอกสารต่าง ๆ ให้หน่วยงานราชการที่เกี่ยวข้อง นอกจากนี้โรงแรมอาจมีแบบฟอร์มอื่น ๆ ที่ลูกค้าอาจต้องกรอก หรือลงนามยินยอมรับทราบในนโยบายต่าง ๆ ที่โรงแรม
- 3) กระบวนการระหว่างการเข้าพัก ช่วงเวลาที่ลูกค้าใช้บริการต่าง ๆ ภายในโรงแรม ทั้งห้องพัก ห้องอาหารโรงแรมหรือร้านอาหารในพื้นที่ สระว่ายน้ำ ห้องออกกำลังกาย สปา กระบวนการทาง

ทะเล หรือกระบวนการท่องเที่ยวเกี่ยวกับผู้ให้บริการในพื้นที่ เช่น แหล่งท่องเที่ยว แหล่งบันเทิง หรือการเดินทางเที่ยวเกาะต่าง ๆ ทริปครึ่งวันไปดำน้ำเกาะต่าง ๆ ในบริเวณใกล้เคียง เป็นต้น

- 4) กระบวนการการเช็คเอาท์ ที่มีขั้นตอนการชำระเงินผ่านทางช่องทางต่าง ๆ มากมาย ไม่ว่าจะเป็นการชำระเงินโดยตรงกับโรงแรมด้วยเงินสด บัตรเครดิต โอนชำระผ่านคิวอาร์โค้ด หรือ Payment Link ต่าง ๆ
- 5) กระบวนการหลังเช็คเอาท์ การติดตามจากฝ่ายการตลาดของโรงแรมที่อาจมีการส่งอีเมลหรือจดหมายขอบคุณ หรือส่งรูปที่ระลึกทางอิเล็กทรอนิกส์ไปให้ลูกค้าพร้อมแนบคู่มือบางส่วนลดสำหรับการเข้าพักครั้งต่อไป

ในการวิเคราะห์กระบวนการที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ เก็บรักษา เปิดเผย ข้อมูลส่วนบุคคล หากจะให้ครอบคลุมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โรงแรมควรเริ่มพิจารณาจากการเก็บรวบรวม เก็บรักษา การใช้ เปิดเผย และการทำลายข้อมูลส่วนบุคคล เพื่อที่จะสามารถเห็นภาพทั้งกระบวนการและสามารถปิดช่องโหว่ทางกฎหมายคุ้มครองและความเสี่ยงที่อาจเกิดการละเมิดข้อมูลส่วนบุคคลได้

ผู้มีส่วนเกี่ยวข้องในธุรกิจโรงแรม



ภาพแสดงบุคคลที่เกี่ยวข้องกับธุรกิจโรงแรมและที่พัก

ทั้งนี้ สถาบันเล็งเห็นความสำคัญของทุก ๆ ส่วนที่เกี่ยวข้องในธุรกิจที่พักและโรงแรม และเป็นกลุ่มผู้ที่ต้องมีความสอดคล้องในการบริหารงาน และดำเนินการให้ตรงตามหลักการของ พรบ.การคุ้มครองข้อมูลส่วนบุคคล

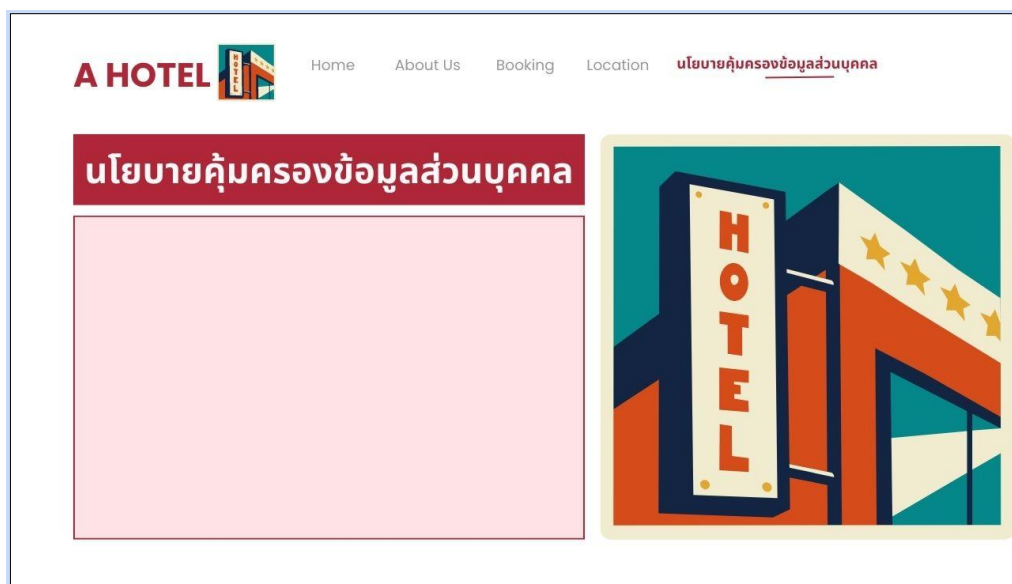
บุคคล พ.ศ. 2562 ด้วยเช่นกัน หากแต่ด้วยข้อจำกัดด้านต่าง ๆ ในแนวปฏิบัตินี้ จะได้หยิบยกประเด็นที่เกี่ยวข้องกับกระบวนการของลูกค้าและการให้บริการต่าง ๆ ที่เกี่ยวข้องกับลูกค้าเท่านั้น

3.2.1 กระบวนการการรับการจอง (Reservation Process)

กระบวนการการรับจอง คือ กระบวนการที่เมื่อลูกค้าค้นหาที่พักและมีการเปรียบเทียบราคาแล้ว ได้ตัดสินใจจองที่พัก โดยทั่วไปแล้ว วิธีการจองสามารถแบ่งออกได้เป็น 4 ประเภท ได้แก่

1. การจองผ่านเว็บไซต์ของโรงแรม ในบางโรงแรมอาจมีการจัดทำเว็บไซต์ของตัวเองเพื่อความสะดวกและเพื่อรองรับปริมาณของลูกค้าที่เข้ามา โดยกระบวนการนี้เป็นกระบวนการที่ทางโรงแรมได้มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าครั้งแรก ดังนั้น ที่หน้าเว็บไซต์โรงแรม ควรมีประกาศความเป็นส่วนตัวเพื่อแจ้งรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าทราบ โดยมีรายละเอียดขั้นต่ำ ได้แก่

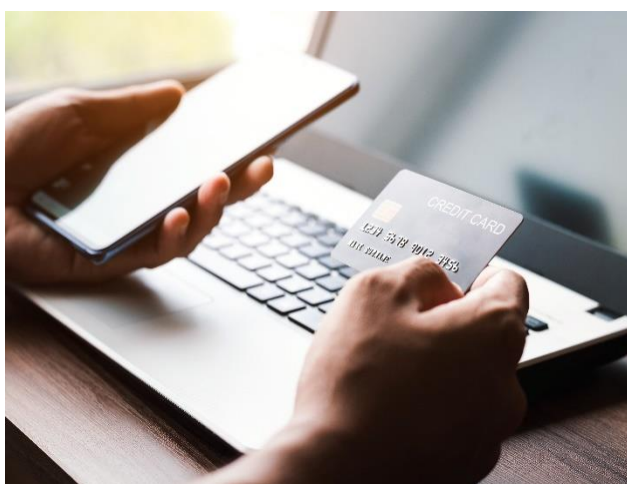
- 1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามกฎหมาย ที่ให้อำนาจในการเก็บรวบรวมได้
- 2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติ ตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
- 3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้
- 4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- 5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณี ที่มีตัวแทนหรือเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของ ตัวแทนหรือเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคลด้วย
- 6) สิทธิของเจ้าของข้อมูลส่วนบุคคลที่มีตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล



ภาพแสดงตัวอย่างการแจ้งประกาศความเป็นส่วนตัวที่หน้าเว็บไซต์โรงแรม

โดยทั่วไปแล้วข้อมูลที่มีการเก็บในกระบวนการการรับรอง เช่น ชื่อ นามสกุล เบอร์ติดต่อ อีเมล ข้อมูลทางการเงินกรณีที่มีการชำระล่วงหน้าหรือมัดจำ ข้อมูลความต้องการพิเศษ รายละเอียดการจอง เป็นต้น ในการจัดเก็บ โรงแรมต้องคำนึงถึงหลักการใช้ข้อมูลอย่างจำกัด (Data Minimization) คือ เก็บเฉพาะข้อมูลที่ต้องใช้ในขั้นตอนการรับรองห้องพักเท่านั้น

โรงแรมควรหลีกเลี่ยงการเก็บข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) เช่น ข้อมูลการแพ้ ข้อมูลความพิการในขั้นตอนการจองห้องพัก เพราะจะเป็นการเพิ่มภาระในการจัดเก็บหากโรงแรมไม่มีความ



จำเป็นต้องประมวลผลข้อมูลเหล่านั้น แต่ถ้าโรงแรมมีความจำเป็นที่จะต้องจัดเก็บ ควรมีการขอความยินยอมลูกค้าก่อนหรือขณะที่เก็บข้อมูล กรณีที่ไม่สามารถหาฐานทางกฎหมายมารองรับการประมวลผลได้ ในการเก็บข้อมูลในขั้นตอนนี้ ถ้าข้อมูลไม่ใช่ข้อมูลอ่อนไหว โรงแรมสามารถใช้ฐานสัญญาในการจัดเก็บข้อมูลได้ เนื่องจากการดำเนินการตามสัญญาเพื่อเข้าพักที่เกิดขึ้นระหว่างลูกค้า และโรงแรมในระบบการรับรองของโรงแรม

อาจมีระบบ Payment Gateway หรือระบบที่รวบรวมและโอนเงินจากลูกค้าไปยังโรงแรม หรือก็คือตัวกลางทางธุรกิจระหว่างลูกค้ากับโรงแรม โดยบริษัทที่ให้บริการ Payment Gateway อาจมีการแลกเปลี่ยนข้อมูลกันระหว่างโรงแรม ดังนั้น โรงแรมควรมีการทำสัญญาการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement : DSA) โดยอาจเพิ่มเนื้อหาเข้าไปในสัญญา หรือ แแนทท้ายสัญญา ที่มีการทำระหว่างบริษัทที่ให้บริการ Payment Gateway ทั้งนี้เพื่อช่วยให้คู่สัญญาทราบถึงบทบาทและหน้าที่ของตนเองเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล การกำหนดวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล รวมถึงการกำหนดมาตรฐานในการแบ่งปันข้อมูลส่วนบุคคล โดยรายละเอียดของข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล ควรมีรายละเอียดขั้นต่ำ ดังนี้

- 1) ชื่อคู่สัญญา/คู่ความร่วมมือ
- 2) วัตถุประสงค์ของการแบ่งปันข้อมูล ซึ่งควรระบุถึงที่มา ความจำเป็น และประโยชน์ที่จะได้รับจากการแบ่งปันข้อมูลส่วนบุคคล
- 3) หน่วยงานอื่นนอกจากคู่สัญญาตามข้อ 1 ที่เข้ามามีบทบาทในการแบ่งปันข้อมูล (ถ้ามี)
- 4) รายละเอียดของข้อมูลส่วนบุคคลที่มีการแบ่งปัน/แลกเปลี่ยน (Data Specification)
- 5) ฐานการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) ทั้งข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลประเภทอ่อนไหว

- 6) ข้อตกลงหรือข้อกำหนดในส่วนที่เกี่ยวกับการใช้ข้อมูลส่วนบุคคลอื่นใด
- 7) ข้อตกลงในส่วนที่เกี่ยวข้องกับการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- 8) ข้อตกลงในส่วนของการบริหารจัดการข้อมูล ตัวอย่างเช่น เงื่อนไขการแบ่งปันข้อมูลระหว่างกัน การบริหารจัดการข้อมูล รูปแบบการบันทึกข้อมูล แนวทางปฏิบัติร่วมกันเรื่องระยะเวลา และการลบทำลาย มาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม และกระบวนการเมื่อสิ้นสุดข้อตกลง เป็นต้น
- 9) เอกสารประกอบที่อาจมี อาทิ แบบฟอร์มการขอใช้ข้อมูล (Data Sharing Request Form) เป็นต้น

2) การจองผ่านช่องทาง Email ในบางโรงแรมอาจมีการรองรับลูกค้าที่จองห้องพักผ่านทางอีเมล ทางโรงแรมควรมีการแจ้งประกาศความเป็นส่วนตัวให้ลูกค้าทราบ โดยอาจแนบประกาศความเป็นส่วนตัวนั้นส่งไปทางอีเมลผู้จองได้ โดยแนบเป็น Link เพื่อให้ลูกค้าสามารถกดเข้าไปอ่านรายละเอียดเกี่ยวกับการจัดเก็บข้อมูลส่วนบุคคลของโรงแรม ในประกาศความเป็นส่วนตัวที่ปรากฏในอีเมลนั้น ต้องมีรายละเอียดขั้นต่ำตามที่กฎหมายกำหนด ตามที่ได้มีการกล่าวมาในข้างต้น โดยอาจใช้ข้อความในลักษณะดังนี้ได้

“โรงแรมเราให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน โปรดอ่านประกาศความเป็นส่วนตัว หรือนโยบายคุ้มครองข้อมูลส่วนบุคคลได้ที่ (แนบ Link)”

3) การจองผ่านทางโทรศัพท์ ในบางโรงแรมอาจมีการรองรับลูกค้าที่จองผ่านการโทรศัพท์ ซึ่งโดยส่วนใหญ่จะเป็นการสอบถามรายละเอียดเกี่ยวกับห้องพัก เมื่อทางผู้จองมีความสนใจจะจอง ทางโรงแรมโดยส่วนใหญ่แล้วจะให้ทางผู้จองแจ้งรายละเอียดผ่านทางอีเมล ซึ่งกระบวนการดำเนินการก็จะเป็นดังข้อ 2) คือ ทางโรงแรมควรมีการแจ้งประกาศความเป็นส่วนตัวให้ลูกค้าทราบ โดยอาจแนบประกาศความเป็นส่วนตัวนั้นส่งไปทางอีเมลได้ โดยแนบเป็น Link เพื่อให้ลูกค้าสามารถกดเข้าไปอ่านรายละเอียดเกี่ยวกับการจัดเก็บข้อมูลส่วนบุคคลของโรงแรม ในประกาศความเป็นส่วนตัวที่ปรากฏในอีเมลนั้น ต้องมีรายละเอียดขั้นต่ำตามที่กฎหมายกำหนด ตามที่ได้มีการกล่าวมาในข้างต้น

4) กรณีการจองผ่าน OTA และ ตัวแทนรับจองทั่วไป กรณีที่เป็นการรับจองผ่านทางตัวแทนรับจอง (Agent) โดยจะมีอยู่ 2 รูปแบบ คือ ตัวแทนรับจองทั่วไป (Traditional Agent) และตัวแทนรับจองออนไลน์ (Online Travel Agent: OTA) เนื่องจากโรงแรมไม่ได้เก็บข้อมูลด้วยตัวเองและมีการแลกเปลี่ยนข้อมูลส่วนบุคคลของผู้จอง โรงแรมกับตัวแทนรับจองควรมีการจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคลด้วย (Data Sharing Agreement: DSA) รวมถึงมีการแจ้งประกาศความเป็นส่วนตัว ตามรายละเอียดที่ได้กล่าวมาในข้างต้นด้วย

5) กรณีติดต่อจองที่โรงแรมโดยตรง (Walk-in) ผู้เข้าประเภท walk-in ส่วนใหญ่ต้องการหาที่พักแบบกะทันหัน ไม่ได้เตรียมตัวมาพักล่วงหน้า ซึ่งจะใช้เวลาในการตัดสินใจจองห้องพักค่อนข้างสั้น เนื่องจากไม่อยากจะเสียเวลาเดินทางไปหาที่พักอื่น ๆ ซึ่งอาจจะต้องดูปัจจัยหลายอย่างประกอบ เช่น ราคา และทำเล แยกประเภทนี้ไม่ค่อยมีเวลาศึกษาข้อมูลมากนัก ทางโรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัว (Privacy

Notice) ให้ผู้เข้าพักทราบ เพื่อแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล โดยอาจแจ้งผ่านหน้าเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ผู้เข้าพักทราบ ทั้งนี้ ขึ้นอยู่กับความสะดวกของโรงแรม

ในกรณีที่ลูกค้ามีการจอง (Reservation) และยืนยันการจอง (Confirmed Booking) การดำเนินการต่อไปคือ กระบวนการก่อนเข้าพัก (Pre-Arrival) ซึ่งในห้วงเวลาระหว่างนี้ ถึง Check-in Process แต่หากลูกค้าทำการยกเลิกการจองห้องพัก เอกสารหรือข้อมูลส่วนบุคคลที่โรงแรมมีการเก็บนั้นควรพิจารณากรอบความจำเป็นในการเก็บ ว่ามีระยะเวลาเท่าใด และหากไม่มีความจำเป็นแล้ว โรงแรมต้องทำลายเอกสารหรือข้อมูลดังกล่าวทิ้ง ซึ่งข้อมูลที่โรงแรมจัดเก็บโดยทั่วไปจะมีด้วยกัน 2 รูปแบบ คือเอกสารกระดาษ อาจกำหนดการทำลายด้วยเครื่องย่อยกระดาษ การเผา หรือการส่งให้บริษัทที่ทำหน้าที่ทำลายเอกสาร ส่วนกรณีเอกสารอิเล็กทรอนิกส์อาจใช้วิธีการลบ หรือทำให้เป็นข้อมูลนิรนาม ที่ไม่สามารถระบุตัวบุคคลได้

3.2.2 กระบวนการการรับที่สนามบิน (Pick-up service activity)

หลังจากที่มีการจองที่พักแล้ว ผู้เข้าพักบางท่านอาจมีความต้องการใช้บริการรถรับส่งเพื่อได้รับจากสนามบินมายังโรงแรมเพื่อความสะดวกของผู้เข้าพัก กระบวนการรับที่สนามบินโดยทั่วไปสามารถแบ่งออกได้เป็น 2 รูปแบบ ได้แก่

- 1) Inhouse limousine คือ กรณีที่โรงแรมมีบริการรับส่งด้วยตัวเอง
- 2) Outsource limousine คือ กรณีที่โรงแรมมีการจ้างบริษัทรับส่งภายนอก ให้ดำเนินการรับส่งผู้เข้าพักแทนโรงแรม

ในกรณีที่โรงแรมมีการจ้างบริษัทรับส่งภายนอก ให้ดำเนินการรับส่งผู้เข้าพักแทนโรงแรม หรือ Outsource limousine ทางโรงแรมอาจมีการส่งรายชื่อของผู้ที่จะเข้าพักให้กับ Outsource limousine ซึ่งเป็นนิติบุคคลภายนอก เช่น ข้อมูล ชื่อ นามสกุล รายละเอียดการเดินทางและการเข้าพัก เป็นต้น การที่โรงแรมมีการจ้างบริษัทภายนอกให้ดำเนินการด้านการรับส่ง บริษัทรับส่งนั้นทำตามภายในนามหรือภายใต้คำสั่งโรงแรมนั้น บริษัท Outsource limousine จึงมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินการตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล ดังนั้น ระหว่าง โรงแรมกับบริษัท Outsource limousine ควรมีการทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) ทั้งนี้เพื่อช่วยให้อุสสัญญาซึ่งเป็นผู้ประมวลผล ทราบถึงบทบาทและหน้าที่ของตนเองเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล การกำหนดวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล การกำหนดมาตรฐานในการแบ่งปันข้อมูลส่วนบุคคล และขอบเขตในการประมวลผลข้อมูลส่วนบุคคล โดยรายละเอียดของข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล ควรมีรายละเอียดขั้นต่ำ ดังนี้

- นิยาม (Definition)
- สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลต่อผู้ประมวลผลและข้อกำหนดห้ามไม่ให้ผู้ประมวลผลทำการนอกเหนือจากคำสั่ง
- ข้อสัญญาเกี่ยวกับหน้าที่รักษาความลับ
- ข้อสัญญาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ข้อสัญญาเกี่ยวกับผู้ประมวลผลช่วง (Sub-Processor)
- ข้อสัญญากำหนดหน้าที่ผู้ประมวลผลในการช่วยเหลือผู้ควบคุมข้อมูลให้ปฏิบัติหน้าที่ตามกฎหมาย
- ข้อสัญญาเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
- ข้อสัญญาเกี่ยวกับการลบหรือส่งคืนข้อมูลส่วนบุคคล

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) นี้ โรงแรมอาจกำหนดไว้เป็นส่วนหนึ่งของสัญญา (Clause) ในสัญญาหลักหรือจัดทำเป็นสัญญาใหม่อีกหนึ่งฉบับ แยกจากสัญญาหลัก หรือจัดทำเป็นข้อตกลงแนบท้าย (Annex) สัญญาพื้นฐานที่มีอยู่เดิมระหว่างโรงแรมและบริษัท Outsource limousine

กรณี บริษัท Outsource limousine มี การรับส่งผู้เข้าพักนอกเหนือจากการรับส่งจากสนามบินมาโรงแรม หรือ บริการรายชั่วโมงหรือบริการแบบเหมา (By-hour) ในกรณีนี้บริษัท Outsource limousine มีอำนาจกำหนดและตัดสินใจเกี่ยวกับการประมวลผลได้เอง ในกิจกรรมที่ทำนอกเหนือจากที่สัญญาประมวลผลไว้ บริษัท Outsource limousine จึงมีสถานะเป็นผู้ควบคุมข้อมูล ดังนั้น โรงแรมจึงต้องมีการกำหนดขอบเขตในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ไว้อย่างชัดเจน เพื่อเป็นการปกป้องผลประโยชน์ของโรงแรม

ทั้งนี้ นอกจากข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) สิ่งที่โรงแรมควรให้ความสำคัญคือโรงแรมควรมีการตรวจสอบเรื่องมาตรการคุ้มครองข้อมูลจากคู่ค้าที่จะเข้าเป็นผู้ประมวลผลว่าบริษัทดังกล่าวมีมาตรการในการคุ้มครองข้อมูลที่เพียงพอ เนื่องจากเป็นเรื่องสำคัญที่ผู้ประกอบการโรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคล เพราะจะส่งผลต่อความน่าเชื่อถือและความไว้วางใจของเจ้าของข้อมูลส่วนบุคคลในบริการขององค์กร รวมถึงเพื่อเป็นการป้องกันการรั่วไหล การล่วงละเมิดข้อมูลส่วนบุคคลด้วย

ในการคัดเลือกบริษัท Outsource limousine โรงแรมควรคัดเลือกคู่ค้าหรือผู้ให้บริการ (Vendor Assessment) เพื่อเลือกคู่ค้าหรือผู้ให้บริการที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ โดย จะต้องพิจารณาคุณสมบัติ 5 ประเด็น ได้แก่

- องค์กร (Organization)
- การดำเนินงาน (Operations)
- ข้อมูล (Data)
- การเข้าถึงข้อมูล (Access)

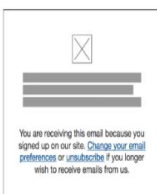
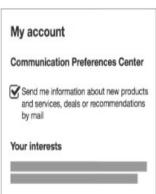
- การปฏิบัติตามกฎหมาย (Compliance)

โดยโรงแรมอาจพิจารณาการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท Outsource limousine โดยมีการจัดทำแบบสอบถามด้านการคุ้มครองข้อมูลส่วนบุคคล และบริษัท Outsource limousine ไม่จำเป็นต้องได้รับความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อการประเมินที่เข้ารับการคัดเลือกเพื่อการจัดซื้อจัดจ้าง เนื่องจากการประเมินทำไปเพื่อการเข้าทำสัญญาระหว่างโรงแรมและบริษัท Outsource limousine แต่ถ้าโรงแรมต้องการประมวลผลข้อมูลส่วนบุคคล นอกเหนือจากวัตถุประสงค์เพื่อการเข้าทำสัญญาจัดซื้อจัดจ้าง หรือเก็บข้อมูลส่วนบุคคลไว้เพื่อใช้ในอนาคต โรงแรมจำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือจะต้องเป็นประโยชน์อันชอบธรรมด้วยกฎหมาย

3.2.3 กระบวนการลงทะเบียนเข้าพัก (Checked-in Process)

กระบวนการลงทะเบียนเข้าพัก (Checked-in Process) คือขั้นตอนที่ต่อเนื่องจาก กระบวนการการจอง (Reservation Process) กระบวนการจะเริ่มขึ้นเมื่อนักท่องเที่ยวทำการลงทะเบียนเข้าพักไปจนถึงนักท่องเที่ยวเข้าพักในการเก็บข้อมูลการลงทะเบียนเข้าพัก โดยทั่วไปแล้วข้อมูลที่มีการจัดเก็บในกระบวนการนี้ เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน/เลขหนังสือเดินทาง อีเมล หมายเลขโทรศัพท์ ช่วงเวลาการเข้าพัก และการเดินทาง หลักฐานการโอนเงิน ข้อมูลบัตรเครดิต ข้อมูลการแพทย์ทางร่างกายและอาหารที่แพ้ ข้อมูลโรคสภาพความพิการ เป็นต้น

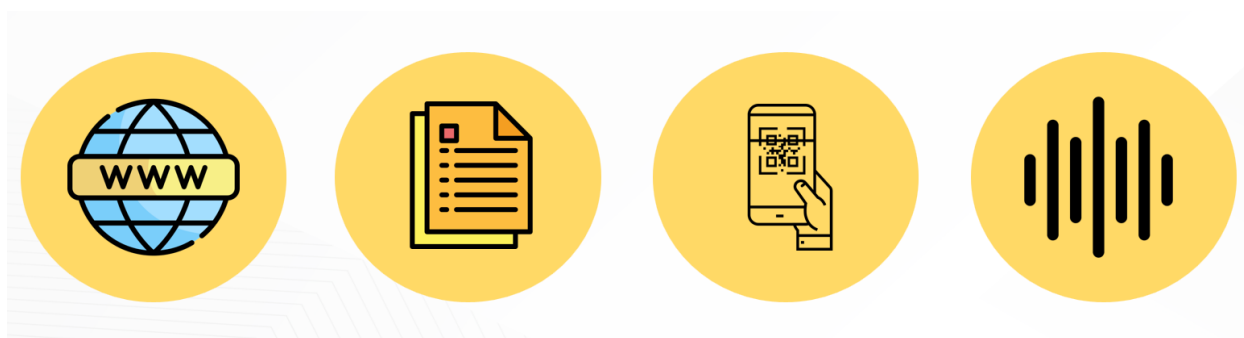
ในการจัดเก็บข้อมูลทางโรงแรมสามารถใช้ฐานสัญญา ในการเก็บรวบรวมข้อมูลส่วนบุคคลทั่วไปของนักท่องเที่ยว เนื่องจากการดำเนินการตามสัญญาใช้บริการ ในส่วนข้อมูลที่มีความอ่อนไหว (Sensitive data) เช่น ข้อมูลการแพ้ ข้อมูลโรค ซึ่งเป็นข้อมูลสุขภาพ โรงแรมควรใช้ฐานความยินยอม (Consent) การขอความยินยอม นั้นอาจทำเป็นเอกสารกระดาษหรือรูปแบบอิเล็กทรอนิกส์ก็ได้ ควรขอความยินยอมเจ้าของข้อมูลก่อนหรือขณะที่ลูกค้าทำการลงทะเบียนเข้าพัก ต้องมีการแจ้งวัตถุประสงค์ในการเก็บที่ชัดเจน ต้องใช้รูปแบบของข้อความที่เข้าใจง่าย ต้องให้ความอิสระกับผู้เข้าพักโดยไม่เป็นการบังคับให้ต้องเลือกหรือเป็นการเลือกไว้แล้วล่วงหน้า ต้องไม่มีเงื่อนไขในการให้บริการ และต้องแจ้งผลกระทบการถอนความยินยอม

Pre-tix box		อิสระในการให้ความยินยอม		แยกส่วนจากเงื่อนไขอื่นๆ	
					

ภาพแสดงตัวอย่างการขอความยินยอมที่ถูกต้อง

นอกจากหนังสือขอความยินยอมแล้ว ทางโรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัว (Privacy Notice) ให้ผู้เข้าพักทราบในจุดต่าง ๆ เพื่อแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล โดยอาจแจ้งผ่านหน้าเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ผู้เข้าพักทราบ ทั้งนี้ขึ้นอยู่กับความสะดวกของโรงแรม โดยต้องมีรายละเอียดขั้นต่ำที่กฎหมายกำหนด ได้แก่

- 1) วัตถุประสงค์ของการเก็บรวบรวม ใช้ เปิดเผย
- 2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติ ตามกฎหมาย หรือสัญญาหรือรวมทั้งแจ้งถึง ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูล
- 3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้
- 4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- 5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ
- 6) สิทธิของเจ้าของข้อมูลส่วนบุคคล



เว็บไซต์

ป้ายประกาศ

QR Code

ข้อความเสียง

ภาพแสดงตัวอย่างช่องทางการแจ้งประกาศความเป็นส่วนตัว

ในบางโรงแรมอาจมีการเก็บข้อมูลศาสนา โดยขอบัตรประชาชนผู้เข้าพักและทำการถ่ายเอกสารบัตรประชาชนซึ่งอาจมีข้อมูลศาสนาติดไปด้วย ซึ่งข้อมูลศาสนานี้ถือว่าเป็นข้อมูลอ่อนไหว (Sensitive data) การประมวลผลต้องขอความยินยอมหากไม่สามารถหาฐานทางกฎหมายอื่นมารองรับได้ หากโรงแรมยังจำเป็นต้องเก็บรวบรวม โรงแรมควรมีมาตรการให้มีการเซ็นหรือขีดกำกับแจ้งวัตถุประสงค์ของเจ้าของข้อมูลก่อน แต่หากไม่มีความจำเป็นต้องเก็บข้อมูลในส่วนนี้ควรมีการขีดฆ่าหรือถมดำก่อนที่จะมีการจัดเก็บข้อมูลดังกล่าว

ในการเก็บรักษา โดยส่วนใหญ่ข้อมูลที่มีการจัดเก็บจะมีทั้งรูปแบบอิเล็กทรอนิกส์และรูปแบบกระดาษ ในส่วนรูปแบบอิเล็กทรอนิกส์นั้นโรงแรมอาจมีการใช้ระบบจัดการข้อมูล โรงแรมควรมีการกำหนดสิทธิการเข้าถึงข้อมูลให้พนักงานแต่ละคน เพื่อป้องกันการรั่วไหลของข้อมูล กรณีที่เป็นโรงแรมขนาดเล็กที่ไม่ได้มีการใช้ระบบ เนื่องจากงบประมาณที่จำกัดหรือไม่มีความจำเป็นต้องใช้ อาจมีการกำหนดการเข้าถึงโดยใช้การตั้ง

๕.๕. ๓

บัตรทะเบียนผู้พักโรงแรม.....

ชื่อตัว ชื่อสกุล

วัน เดือน ปี เกิด

อาชีพ สัญชาติ

ที่อยู่ปัจจุบัน หมายเลขโทรศัพท์

(บ้านเลขที่ ตำบล อำเภอ จังหวัด ประเทศ)

มาจาก

จะไปที่

(บ้านเลขที่ ตำบล อำเภอ จังหวัด ประเทศ)

เลขประจำตัวประชาชน

บัตรประจำตัวประชาชนออกให้โดย..... วันออกบัตร..... บัตรหมดอายุ.....

ใบสำคัญประจำตัวคนต่างด้าวเลขที่..... ออกให้โดย.....

หนังสือเดินทางเลขที่..... ออกให้โดย.....

วัน เดือน ปี ที่เข้ามาพัก	วัน เดือน ปี ที่ออกไป	ห้องพักเลขที่ ลายมือชื่อผู้พัก
เวลา	เวลา	

ภาพแสดงตัวอย่าง แบบฟอร์มใบ ร.ร. 3

ซึ่งโดยส่วนใหญ่โรงแรมจะทำการพิมพ์แบบฟอร์ม ร.ร. 3 เพื่อให้ผู้เข้าพักทำการกรอกรายละเอียดเอง จากนั้นโรงแรมจะนำข้อมูลดังกล่าวกรอกในแบบ ร.ร. 4 ซึ่งเป็นแบบฟอร์มทะเบียนผู้พักโรงแรม ซึ่งโรงแรมมีหน้าที่ ผู้จัดการต้องส่งสำเนาทะเบียนผู้พัก (ร.ร. 4) ในแต่ละวันไปให้นายทะเบียนทุกสัปดาห์แล้วให้นายทะเบียนทำใบรับมอบให้ไว้เป็นสำคัญ หากโรงแรมอยู่ห่างไกลหรือไม่สามารถส่งได้ตามกำหนดดังกล่าว ให้นายทะเบียนพิจารณากำหนดระยะเวลาส่งสำเนาดังกล่าวและแจ้งให้ผู้จัดการทราบ โดยข้อมูลที่มีการเก็บใน ร.ร. 4 ได้แก่ วันที่เข้าพัก ชื่อนามสกุล สัญชาติ เลขประจำตัวประชาชนหรือเลขพาสปอร์ต ที่อยู่ อาชีพ รายละเอียดการเดินทาง

ร.ร. ๓

ทะเบียนผู้พักในโรงแรม.....

GUEST REGISTRATION FORM OF

ประจำวันที่ เดือน พ.ศ. ถึงวันที่ เดือน พ.ศ.

FROM: DATE.....MONTH.....YEAR..... TO DATE.....MONTH.....YEAR.....

ลำดับ No.	วันที่เข้าพัก Date and Time of Arrival	ห้องพัก เลขที่ Room No.	ชื่อตัวและชื่อสกุล Guest Name	สัญชาติ Nationality	เลขบัตรตัวและเลขหนังสือ ในต่างประเทศ หรือบัตรการขึ้นที่ พำนักในถิ่น Identification Card No. or Alien Registration Book No. or Passport No.	ที่อยู่ปัจจุบัน Current Address	อาชีพ Occupation	มาจากตำบล อำเภอ จังหวัด หรือประเทศใด Place of Departure	จะไปที ตำบล อำเภอ จังหวัด หรือประเทศใด Next Destination	วันที่ ออกไป Expected Departure	หมายเหตุ Remarks

ขอรับรองว่าเป็นความจริงทุกประการ

(ลงชื่อ).....ผู้จัดการ

ภาพแสดงตัวอย่าง แบบฟอร์มใบ ร.ร. 4

ในการเก็บข้อมูล ร.ร. 3 และ ร.ร. 4 นั้น เป็นการจัดเก็บตามกฎหมาย ได้แก่ พระราชบัญญัติโรงแรม พ.ศ. 2547 ดังนั้น โรงแรมสามารถอ้างฐานปฏิบัติตามกฎหมาย (Legal Obligation) ในการใช้และเปิดเผยนั้น เนื่องจากการเป็นการเป็นการเปิดเผยตามกฎหมายจึงสามารถอ้างฐานการปฏิบัติตามกฎหมายข้างต้นได้ ทั้งนี้ โรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัวให้ผู้เข้าพักทราบเกี่ยวกับการประมวลดังกล่าวด้วย



ในการเก็บรักษา เนื่องจากข้อมูลที่จัดเก็บอาจมีทั้งข้อมูลที่เป็น Hard copy และ Soft file เอกสาร Hard copy โรงแรมควรมีการจัดเก็บในพื้นที่ที่มีการกำหนดการเข้าถึงว่าบุคคลระดับใดบ้างที่เข้าถึงได้และ อาจมีการล็อกกุญแจ ในส่วนเอกสาร Soft file ซึ่งต้องมีการนำส่งกรมการปกครองผ่านทางเว็บไซต์และอาจมีการ เก็บไว้ในฐานข้อมูล โรงแรมควรมีการกำหนดการเข้าถึงของข้อมูล ว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการกำหนดรหัสการเข้าถึงเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

เมื่อนำส่งเอกสารให้กับกรมการปกครองแล้ว เอกสารบัตรทะเบียนผู้พัก (ร.ร. 3) และทะเบียนผู้พัก (ร.ร. 4) โรงแรมต้องมีการเก็บไว้อย่างน้อย 1 ปี เพื่อการตรวจสอบจากกรมการปกครอง เนื่องจากเป็น ระยะเวลาที่กำหนดตามกฎหมาย ตามมาตรา 35 พระราชบัญญัติโรงแรม พ.ศ. 2547 และเมื่อครบกำหนดการ จัดเก็บโรงแรมต้องกำหนดวิธีการทำลายเอกสารให้ชัดเจน เช่น การเผา การลบ การทำให้เป็นข้อมูลนิรนาม หรือการใช้เครื่องย่อยเอกสาร ทั้งนี้ขึ้นอยู่กับความสะดวกของโรงแรม

3.2.5. กระบวนการนำส่ง ตม. 30 ให้สำนักงานตรวจคนเข้าเมือง

เอกสาร ตม. 30 คือ เอกสารที่ใช้แจ้งที่พักของคนต่างด้าว ตามพระราชบัญญัติคนเข้าเมือง พ.ศ. 2522 โดยมาตรา 38 ได้กำหนดไว้ว่า “เจ้าบ้าน เจ้าของบ้านหรือผู้ครอบครองเคหสถาน หรือผู้จัดการโรงแรมซึ่งรับ คนต่างด้าวซึ่งได้รับอนุญาตให้อยู่ในราชอาณาจักรเป็นการชั่วคราว เข้าพักอาศัย จะต้องแจ้งต่อพนักงาน เจ้าหน้าที่ ณ ที่ทำการตรวจคนเข้าเมืองซึ่งตั้งอยู่ในท้องที่ เคหสถาน หรือโรงแรมนั้นอยู่ ภายในยี่สิบสี่ชั่วโมง นับแต่เวลาที่คนต่างด้าวเข้าพักอาศัย ถ้าท้องที่ใดไม่มีที่ทำการตรวจคนเข้าเมืองตั้งอยู่ ให้แจ้งต่อเจ้าพนักงาน ตำรวจ ณ สถานีตำรวจในท้องที่นั้นในกรณีที่บ้าน เคหสถาน หรือโรงแรมที่คนต่างด้าวเข้าพักอาศัย ตามวรรค หนึ่งตั้งอยู่ในเขตท้องที่กรุงเทพมหานคร ให้แจ้งต่อพนักงานเจ้าหน้าที่ ณ กองตรวจคนเข้าเมือง การแจ้งตาม วรรคหนึ่งและวรรคสองให้เป็นไปตามระเบียบที่อธิบดีกำหนด”

ในการแจ้งที่พักคนต่างด้าวที่เข้าพักอาศัยในเคหสถานซึ่งได้แก่ โรงแรมที่ได้รับอนุญาตตาม พระราชบัญญัติโรงแรม พ.ศ. 2547 และเกสเฮาส์ แมนชั่น อพาร์ทเมนต์ สถานประกอบการหรือบ้านเช่าทั่ว ๆ ไป ให้เจ้าของเคหสถานดังกล่าว เจ้าของบ้านเช่า หรือผู้ประกอบการแจ้งตามแบบ ตม. 30 สำนักงานตรวจคน เข้าเมืองได้กำหนดรูปแบบและวิธีให้บริการเพื่อผู้มาขอรับบริการได้เลือกวิธีการที่เหมาะสมสำหรับการ ดำเนินการดังนั้นเอกสารแบบ ตม. 30 มาแจ้งด้วยตนเอง หรือมอบหมายให้ผู้อื่นนำเอกสารมาแจ้ง หรือ แจ้ง ทางไปรษณีย์ลงทะเบียน หรือแจ้งทางระบบอินเทอร์เน็ต (Internet)

ข้อมูลส่วนบุคคลที่มีการเก็บใน ตม. 30 ที่กฎหมายกำหนด ได้แก่ ชื่อ นามสกุล เลขหนังสือเดินทาง สัญชาติ เพศ วันเดือนปีเกิด วันเดินทางเข้าประเทศ ประเภทหนังสือเดินทางและวันหมดอายุ ช่องทางการเข้า ประเทศ เลขที่บัตรขาเข้าประเทศ ในการเก็บข้อมูลในเอกสาร ตม. 30 เป็นการจัดเก็บตามกฎหมาย คือ ตาม พระราชบัญญัติ คนเข้าเมือง พ.ศ. 2522 ดังนั้น โรงแรมสามารถอ้างฐานปฏิบัติตามกฎหมาย (Legal Obligation) ในการใช้และเปิดเผยนั้น เนื่องจากเป็นการเป็นการเปิดเผยตามกฎหมายจึงสามารถอ้างฐานการ ปฏิบัติตามกฎหมายข้างต้นได้ ทั้งนี้ โรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัวให้ผู้เข้าพักทราบเกี่ยวกับ วัตถุประสงค์การประมวลนี้ด้วย

ในการเก็บรักษา เนื่องจากข้อมูลที่จัดเก็บอาจมีทั้งข้อมูลที่เป็น Hard copy และ Soft file เอกสาร Hard copy โรงแรมควรมีการจัดเก็บในพื้นที่ที่มีการกำหนดการเข้าถึงว่าบุคคลระดับใดบ้างที่เข้าถึงได้และ อาจมีการล็อกกุญแจ ในส่วนเอกสาร Soft file ซึ่งต้องมีการนำส่งกรมการปกครองผ่านทางเว็บไซต์และอาจมีการเก็บไว้ในฐานข้อมูล โรงแรมควรมีการกำหนดการเข้าถึงของข้อมูล ว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการกำหนดรหัสการเข้าถึงเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

เมื่อนำส่งเอกสารให้กับสำนักงานตรวจคนเข้าเมือง (สตม.) แล้ว ตม. 30 กฎหมายมิได้กำหนดระยะเวลาที่ชัดเจนว่าต้องเก็บกี่ปี ดังนั้น อาจใช้เทียบระยะเวลาการจัดเก็บตามเอกสาร ร.ร. 3 และ ร.ร. 4 ได้ กล่าวคือโรงแรมควรมีการเก็บไว้อย่างน้อย 1 ปี เพื่อการตรวจสอบ ทั้งนี้ หากโรงแรมต้องการเก็บนานกว่านั้น ย่อมสามารถทำได้ แต่ต้องมีเหตุผลจำเป็นที่ใช้อ้างอิงกับตัวเจ้าของข้อมูลหรือหน่วยงานกำกับดูแลกรณีเกิดการตรวจสอบขึ้นมา โดยโรงแรมอาจอ้างเหตุผลในการจัดเก็บ เช่น เหตุผลในการก่อตั้งสิทธิ การร้องเรียน หรือเพื่อการฟ้องร้องหรือใช้อำนาจศาล เป็นต้น และเมื่อครบกำหนดการจัดเก็บโรงแรมต้องกำหนดวิธีการทำลาย เอกสารให้ชัดเจนว่าจะทำลายด้วยวิธีใด เช่น การเผา การลบ การทำให้เป็นข้อมูลนิรนาม หรือการใช้เครื่องย่อยเอกสาร ทั้งนี้ขึ้นอยู่กับความสะดวกของโรงแรม

พ.ม.๕๐
TM.30

แบบการแจ้งคนต่างด้าวเข้าพักอาศัย สำหรับเจ้าของบ้าน เจ้าของหรือผู้ครอบครองสถานที่ หรือผู้จัดการโรงแรม
NOTIFICATION FORM FOR HOUSE-MASTER, OWNER OR POSSESSOR OF RESIDENCE
OR HOTEL MANAGER WHERE ALIEN HAS STAYED

เขียนที่.....
Written at

วันที่ เดือน ปี ค.ศ.
Date Month Year

เรียน พนักงานเจ้าหน้าที่ตรวจคนเข้าเมือง
To: The Immigration Officer

ข้าพเจ้า..... อายุ..... ปี
I..... Age Years

สัญชาติ..... สัญญาบัตร..... เลขที่.....
Nationality Present Address Lane

ถนน..... อำเภอ/เขต.....
Road Tambon/Khwaeng (Subdistrict) Amphoe/Phet (District)

จังหวัด..... ขอแจ้งการพักอาศัยของบุคคลต่างด้าวในบางช่วงในราชอาณาจักรไทย
Changwat (Province) wish to notify the address where alien receiving permission

เป็นการชั่วคราว ซึ่งจำอยู่ที่..... ขอ.....
To stay temporarily in the kingdom has stayed as follows Lane

ถนน..... อำเภอ/เขต.....
Road Tambon/Khwaeng (Subdistrict) Amphoe/Phet (District)

จังหวัด..... เดือน..... ปี ค.ศ.....
Changwat (Province) On Date Month Year

รวม..... คน (ตามบัญชีแนบมาด้วย)
Total Person(s) (Name list Attached)

ลงชื่อ..... ผู้ได้รับอนุญาตเข้าบ้าน เจ้าของ หรือผู้ครอบครองสถานที่ หรือผู้จัดการโรงแรม
Signature House-Master, Owner or Possessor of Residence or Hotel Manager

หมายเหตุ
NOTICE

๑. แจ้งภายใน ๒๔ ชั่วโมง นับแต่คนต่างด้าวเข้าพักอาศัย
Must notify within 24 hours from the time of arriving at the residence.

๒. ในเขตกรุงเทพมหานคร ให้แจ้งต่อกองกักกันการตรวจคนเข้าเมือง ๑
In Bangkok area, notify Immigration Division 1.

๓. ในจังหวัดอื่น ให้แจ้งต่อที่การตรวจคนเข้าเมืองซึ่งมีอำนาจขึ้นสืบชอบ
In provincial area, notify authorized provincial Immigration office.

ใบรับทราบแจ้งคนต่างด้าวเข้าพักอาศัย
RECEIPT OF NOTIFICATION

ข้าพเจ้า..... ตำแหน่ง..... สัญชาติ.....
I..... TITLE Nationality

ได้รับทราบแจ้งคนต่างด้าวเข้าพักอาศัยของ.....
Have received notification of alien's address from.....

ซึ่งได้แจ้งการเข้าพักอาศัยของ..... รวม..... คน ไม่ไว้
Who notify residence where alien has stayed Total Person(s)

เมื่อวันที่ เดือน..... ปี ค.ศ..... เวลา..... น.
on date Month Year hours

ลงชื่อ..... ผู้รับแจ้ง
Signature Immigration officer

บัญชีชื่อคนต่างด้าวที่พำนัก
NAME OF ALIENS IN RESIDENCE
(IN BLOCK LETTERS)

ลำดับ NO.	ชื่อคนต่าง Name and Surname	สัญชาติ Nationality	หนังสือเดินทาง Passport Number	ประเภทวีซ่า Type of Visa	วันเข้ามา Date of Arrival	หมดอายุ Expiry Date of Stay	จุดเข้า Point of Entry	บัตรเข้าเมือง Arrival Card TM.30.0	พักอยู่ ระยะยาว ปี..... Period of stay From.....to.....	ความสัมพันธ์ Relationship

ลงชื่อ..... ผู้แจ้ง
Signature

ภาพแสดงตัวอย่าง แบบฟอร์ม ตม. 30

3.2.6 กระบวนการการใช้กล้องวงจรปิด (CCTV Using Process)

โดยทั่วไปแล้วในพื้นที่โรงแรมโดยเฉพาะพื้นที่ส่วนกลาง (Public Area) และพื้นที่ทำงาน (Working Area) จะมีการติดตั้งกล้อง CCTV เพื่อวัตถุประสงค์ในการรักษาความปลอดภัยปกป้องคุ้มครองสุขภาพและความปลอดภัย รวมถึงทรัพย์สินผู้เข้าพัก การเก็บข้อมูลในในกล้อง CCTV เป็นการเก็บข้อมูลส่วนบุคคล เนื่องจาก มีการบันทึกข้อมูลส่วนบุคคล ได้แก่ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ภาพทรัพย์สินของผู้เข้าพัก เช่น ยานพาหนะ เครื่องประดับ กระเป๋า หมวก เครื่องแต่งกาย เป็นต้น

การเก็บข้อมูล CCTV นั้นอาจมีการกำหนดวัตถุประสงค์ในการจัดเก็บหลายวัตถุประสงค์ โรงแรมอาจดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เข้าพักเพื่อวัตถุประสงค์ต่าง ๆ เช่น

- 1) เพื่อการปกป้องสุขภาพและความปลอดภัยส่วนตัวซึ่งรวมถึงทรัพย์สิน
- 2) เพื่อการปกป้องอาคาร สิ่งอำนวยความสะดวกและทรัพย์สินของโรงแรมจากความเสี่ยง การขัดขวาง การทำลายซึ่งทรัพย์สินหรืออาชญากรรมอื่น
- 3) เพื่อสนับสนุนหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายเพื่อการยับยั้ง ป้องกัน สืบค้น และดำเนินคดีทางกฎหมาย
- 4) เพื่อการให้ความช่วยเหลือในกระบวนการระงับข้อพิพาทซึ่งเกิดขึ้นในระหว่างที่มีกระบวนการทางวินัยหรือกระบวนการร้องทุกข์
- 5) เพื่อการให้ความช่วยเหลือในกระบวนการสอบสวน หรือ กระบวนการเกี่ยวกับการส่งเรื่องร้องเรียน
- 6) เพื่อการให้ความช่วยเหลือในกระบวนการริเริ่มหรือป้องกันการฟ้องร้องทางแพ่ง ซึ่งรวมถึงแต่ไม่จำกัดเพียงการดำเนินการทางกฎหมายที่เกี่ยวข้องกับการจ้างงาน

ในการเก็บข้อมูลในกล้อง CCTV โรงแรมสามารถใช้ฐานประโยชน์โดยชอบธรรม (Legitimate Interest) เพื่อประโยชน์โดยชอบด้วยกฎหมายของโรงแรมโดยไม่เกินขอบเขตที่สามารถคาดหมายได้อย่างสมเหตุสมผล ซึ่งจะไม่ละเมิดสิทธิพื้นฐาน หรือสิทธิ ทางเสรีภาพของตัวผู้เข้าพักอาศัย และสามารถใช้นฐานการปฏิบัติตามกฎหมาย (Legal Obligation) กรณีที่เป็นไปเพื่อปฏิบัติหน้าที่ตามที่กฎหมายกำหนด เช่น กฎหมายอาญา กฎหมายแพ่งและพาณิชย์ กฎหมายวิธีพิจารณาความแพ่ง กฎหมายวิธีพิจารณาความอาญา กรณีโอนข้อมูลให้หน่วยงานราชการภายนอก เป็นต้น

การเก็บข้อมูล CCTV นั้น โรงแรมต้องแจ้งประกาศความเป็นส่วนตัว โดยจัดให้มีประกาศแจ้งเตือนการใช้กล้องวงจรปิด (CCTV Notice) เพื่อแจ้งสิทธิแก่ผู้มาติดต่อหรือลูกค้าไว้อย่างชัดเจนเพื่อป้องกันความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยหลักการแจ้ง CCTV Notice ที่ดีสามารถทำได้ดังนี้

1. ภายในประกาศจะต้องระบุไว้อย่างชัดเจนว่า ภายในบริเวณดังกล่าว มีการติดกล้องวงจรปิด ซึ่งเป็นการแจ้งสิทธิพื้นฐานให้แก่ผู้มาติดต่อ หรือผู้มาใช้บริการได้ทราบ และจะต้องติดไว้ในจุดที่สังเกตเห็นได้ง่าย และชัดเจน ใช้ภาษาที่เข้าใจง่าย ไม่กำกวม หรือเจตนาทำให้เข้าใจผิด

2. จัดทำประกาศการคุ้มครองส่วนบุคคลเกี่ยวกับการใช้กล้องวงจรปิด (Privacy Notice on CCTV Use)

ซึ่ง Privacy Notice on CCTV Use จะต้องประกอบด้วย

- 1) ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม คือ บอกข้อมูลว่าเก็บภาพ ภาพนิ่ง หรือเสียง สนทนา อะไรบ้าง
- 2) วิธีการประมวลผลข้อมูลส่วนบุคคล หากมีการจัดเก็บแล้วนำไปใช้ประโยชน์ทางธุรกิจ มีการดำเนินการใดบ้าง
- 3) วัตถุประสงค์ในการเก็บข้อมูลเพื่อนำไปใช้ประโยชน์ด้านใดบ้าง
- 4) หลักเกณฑ์ หรือฐานทางกฎหมาย ว่าโรงแรมในฐานะใดบ้างในการเก็บและประมวลผลข้อมูลลูกค้าจากไฟล์ที่บันทึกโดยกล้องวงจรปิด CCTV เช่น ฐานกฎหมาย ฐานประโยชน์โดยชอบ หรือฐานสัญญา
- 5) ข้อมูลที่มีการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม ควรระบุด้วยว่าข้อมูลจากกล้องวงจรปิดมีการเปิดเผยหรือส่งต่อแก่บุคคลที่สามใดบ้าง และเพื่อกิจกรรมใด
- 6) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล มีการเก็บไว้นานเท่าใด และจะลบทำลายเมื่อใด
- 7) การแจ้งสิทธิ นั่นคือบอกอย่างตรงไปตรงมา โดยการจัดทำสติ๊กเกอร์แจ้งตามที่ระบุข้างต้น (ข้อที่ 1) ทั้งควรจัดทำ QR Code เพื่อเป็นช่องทางให้ลูกค้าสามารถสแกนเพื่อรับทราบสิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคลได้ เช่น สิทธิในการขอให้แก้ไข ขอสำเนา ระงับ ถ่ายโอน หรือลบทำลาย
- 8) ช่องทางการติดต่อของโรงแรม ในกรณีที่ลูกค้าต้องการทราบถึงรายละเอียดอื่นๆ หรือมีคำขอสำหรับการใช้สิทธิโดยชอบตามกฎหมาย PDPA
- 9) มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล โรงแรมจะต้องมีการป้องกันข้อมูลรั่วไหล หรือการละเมิดที่เหมาะสมกับความเสี่ยง



พื้นที่นี้มีการติดตั้งกล้องวงจรปิด ตลอด 24
ชั่วโมง เพื่อการรักษาความปลอดภัย



Scan เพื่ออ่านประกาศความเป็นส่วนตัว

ภาพแสดงตัวอย่างป้ายประกาศ CCTV

ในการจัดเก็บข้อมูล CCTV โรงแรมควรกำหนดระยะเวลาในการเก็บรักษาไฟล์ CCTV ที่มีภาพ ใบหน้า ท่าทาง อากัปกริยา อันเป็นข้อมูลส่วนบุคคลของผู้เข้าพักที่โรงแรม แม้ว่ากฎหมายไม่ได้กำหนดระยะเวลาที่แน่นอน แต่กฎหมายกำหนดไว้ว่า

- โรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้ง ระยะเวลาในการเก็บรวบรวม โดยกำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม เช่น อาจเก็บเท่าที่จำเป็นตามที่กฎหมายกรณีเกิดข้อพิพาทขึ้น หรือ ไม่เกิน 30 45 หรือ 60 วัน
- โรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบตรวจสอบเพื่อลบ หรือทำลายไฟล์เมื่อพ้นกำหนดระยะเวลาที่กล่าวมาข้างต้น หรือกรณีที่ไม่มีเวลาจำเป็นในการเก็บรักษาไฟล์ CCTV อันเป็นส่วนหนึ่งของข้อมูลส่วนบุคคลแล้วโรงแรมต้องทำการ ลบ ทำลายข้อมูลส่วนบุคคลทิ้ง
- โรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการบันทึกระยะเวลาการเก็บรักษาข้อมูลไฟล์ CCTV ว่าจะเก็บไว้นานเท่าใดเพื่อให้ เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

3.2.7 กระบวนการการเปิดสมาชิก (Hotel Member Process)

ระบบสมาชิก (Hotel Member) มีจุดประสงค์เพื่อมอบสิทธิประโยชน์ให้กับลูกค้าที่เพื่อดึงดูดลูกค้าให้ได้อย่างต่อเนื่องและยาวนาน โดยโรงแรมจะมีการติดต่อสื่อสารเกี่ยวกับ Promotion ต่าง ๆ กับลูกค้ากลุ่มเป้าหมายอย่างสม่ำเสมอ ซึ่งในบางโรงแรมการเป็นสมาชิกนั้นทำให้ผู้เข้าพักสามารถใช้สิทธิ์ที่โรงแรมในกลุ่มเครือหรือพันธมิตรอื่น ๆ นอกเหนือไปจากโรงแรมได้

ข้อมูลส่วนบุคคลโดยทั่วไปที่มีการเก็บในกิจกรรมการเปิดสมาชิกนั้น เช่น ชื่อ นามสกุล อีเมล รายละเอียดที่อยู่ รายละเอียดการติดต่อ วันเดือนปีเกิด เป็นต้น โรงแรมควรพิจารณาถึงปริมาณข้อมูลที่มีการเก็บว่าจำเป็นต้องเก็บมากเท่าใด และควรหลีกเลี่ยงการเก็บข้อมูลอ่อนไหว (Sensitive Data) ซึ่งไม่มีความจำเป็นที่ต้องเก็บในกิจกรรมการเปิดสมาชิก มิเช่นนั้น จะเป็นการเพิ่มภาระให้กับโรงแรมและเป็นการผิดหลักการคุ้มครองข้อมูล คือ หลักการใช้ข้อมูลอย่างจำกัด (Data Minimization)

ข้อมูลที่โรงแรมเก็บมานั้น โรงแรมสามารถใช้ฐานสัญญาในการเก็บข้อมูลได้รวมถึงการประมวลผลต่างๆ ตามสัญญาและโรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัวให้เจ้าของข้อมูลทราบ ทางโรงแรมต้องมีการแจ้งประกาศความเป็นส่วนตัว (Privacy Notice) ให้กับสมาชิกทราบ เพื่อแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล ทางโรงแรมอาจแจ้งผ่านหน้าเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ผู้เข้าพักทราบ ทั้งนี้ขึ้นอยู่กับความสะดวกของโรงแรม

ในการเก็บรักษา ข้อมูลที่อยู่ในระบบสมาชิกโรงแรมต้องมีการกำหนดระยะเวลาการจัดเก็บที่เหมาะสมตามวัตถุประสงค์ในการประมวลผลตามสัญญาสมัครสมาชิก และโรงแรมควรมีการกำหนดการเข้าถึงของข้อมูลว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการกำหนดรหัสการเข้าถึงเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

ทั้งนี้ โรงแรมต้องมีการจัดช่องทางการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล โดยผู้เข้าพักมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลในเวลาใดก็ได้ หากการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ที่ทำขึ้นเพื่อการดำเนินงานที่จำเป็นภายใต้ประโยชน์โดยชอบด้วยกฎหมายของโรงแรม หรือของบุคคลหรือนิติบุคคลอื่น โดยไม่เกินขอบเขตที่สมาชิกสามารถคาดหมายได้อย่างสมเหตุสมผล หรือเพื่อดำเนินการตามภารกิจเพื่อสาธารณประโยชน์ หากสมาชิกยื่นคัดค้าน โรงแรมจะต้องแจ้งสมาชิกว่า โรงแรมจะยังคงดำเนินการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปเฉพาะที่โรงแรมสามารถแสดงเหตุผลตามกฎหมายได้ว่ามีความสำคัญยิ่งกว่าสิทธิขั้นพื้นฐานของสมาชิก หรือเป็นไปเพื่อการยืนยันสิทธิตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการต่อสู้ในการฟ้องร้องตามกฎหมาย ตามแต่ละกรณี นอกจากนี้ สมาชิกยังมีสิทธิขอคัดค้านการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของสมาชิกที่สร้างขึ้นเพื่อวัตถุประสงค์เกี่ยวกับการตลาด หรือเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติได้อีกด้วย

เมื่อสิ้นสุดการเป็นสมาชิกแล้ว เอกสารหรือข้อมูลส่วนบุคคลที่โรงแรมมีการเก็บนั้นควรพิจารณากรอบความจำเป็นในการเก็บ ว่ามีระยะเวลาเท่าใด และหากไม่มีความจำเป็นแล้ว โรงแรมต้องทำลายเอกสารหรือข้อมูลดังกล่าวทิ้ง ซึ่งข้อมูลที่โรงแรมจัดเก็บโดยทั่วไปจะมีด้วยกัน 2 รูปแบบ คือเอกสารกระดาษ อาจกำหนดการทำลายด้วยเครื่องย่อยกระดาษ การเผา หรือการส่งให้บริษัทที่ทำหน้าที่ทำลายเอกสาร ส่วนกรณีเอกสารอิเล็กทรอนิกส์อาจใช้วิธีการลบ หรือทำให้เป็นข้อมูลนิรนาม ที่ไม่สามารถระบุตัวบุคคลได้

3.2.8 กระบวนการการชำระค่าบริการโรงแรม (Hotel Payment Process)

โดยทั่วไปแล้ว การชำระเงินของโรงแรม จะมีด้วยกัน 6 วิธีชำระเงิน (Payment) โดยมีรายละเอียดดังนี้

1. เงินสด (Cash)
2. บัตรเครดิต/เดบิต (Credit/Debit Card) โดยโรงแรมจะต้องติดตั้งเครื่องรูดบัตร (EDC) ก่อน ถึงจะสามารถรับบัตรเครดิตได้ ส่วนใหญ่ที่ผู้เข้าพักจะใช้ก็มี วีซ่า มาสเตอร์การ์ด อเมริกันเอ็กซ์เพรส ไดเนอร์คลับ เจซีบี เป็นต้น
3. COA (Cash on Arrival) เป็นวิธีการชำระเงินก่อนที่ผู้เข้าพักจะเข้าพัก บริษัททัวร์ที่ใช้วิธีนี้ จะมีข้อตกลงว่า ถ้าไม่ชำระเงินค่าห้องพักก่อน โรงแรมก็จะไม่ให้กุญแจ ผู้เข้าพักคนนั้นก็ไม่สามารถเข้าพักได้ ส่วนใหญ่แล้วโรงแรมที่มีผู้เข้าพักเป็นบริษัททัวร์มักจะเริ่มต้นสัญญาเป็นการชำระแบบ COA
4. COD (Cash on Departure) เป็นวิธีการชำระเงินที่ตรงข้ามกับ COA เพราะให้ผู้เข้าพักชำระเงินก่อนจะออกจากโรงแรม (Check out) บริษัททัวร์ที่ใช้วิธีนี้ จะมีข้อตกลงว่า ถ้าไม่ชำระเงินค่าห้องพักก่อน Check out ทางโรงแรมจะไม่ให้ผู้เข้าพักออกจากโรงแรม
5. City Ledger วิธีการชำระเงินแบบวางบิลเรียกเก็บกับบริษัท ใช้ได้ทั้งกับบริษัททัวร์ ราชการ และบริษัททั่วไป



6. การโอนเงินผ่านเคาเตอร์เซอร์วิส หรือการชำระเงินผ่านคนกลางทั้งที่เป็นสถาบันการเงินของธนาคารและที่ไม่ใช่สถาบันการเงิน (non-Bank)

ในการเก็บข้อมูลทางการเงิน โดยเฉพาะข้อมูลบัตรเครดิตปัจจุบันโรงแรมอาจมีการให้ผู้เข้าพักกรอกรายละเอียดเกี่ยวกับบัตรเครดิต รวมถึงขอสำเนาบัตรเครดิต เพื่อทำธุรกรรมกับทางโรงแรม เช่น ในขั้นตอนการจ่ายค่ามัดจำ หรือการชำระค่าจองห้องพัก รายละเอียดข้อมูลบัตรเครดิตที่เก็บนั้น เป็นข้อมูลส่วนบุคคลที่มีความสำคัญอย่างมาก เนื่องจากเป็นข้อมูลทางการเงินซึ่งหากเกิดการรั่วไหลขึ้นมาก็จะเกิดความเสียหายต่อตัวเจ้าของข้อมูลได้

ข้อมูลบัตรเครดิตที่มีการเก็บนั้น โรงแรมสามารถอ้างอิงฐานสัญญาได้ เนื่องจากการเก็บข้อมูลดังกล่าวเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา (การชำระค่าห้องพักรวมถึงค่าบริการต่าง ๆ ระหว่างเข้าพักในโรงแรม) แม้ว่าจะมีฐานทางกฎหมายเพื่อเก็บข้อมูลแล้วก็ตาม โรงแรมเองก็ต้องมีการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลบัตรเครดิตให้ผู้เข้าพักซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลทราบด้วย ก่อนหรือขณะที่มีการเก็บข้อมูลส่วนบุคคลทางโรงแรมอาจแจ้งผ่านเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ผู้เข้าพักทราบ ทั้งนี้ขึ้นอยู่กับความสะดวกหรือแนวการปฏิบัติของโรงแรม

โรงแรมต้องมีการกำหนดวิธีในการเก็บรักษา เนื่องจากข้อมูลที่จัดเก็บอาจมีทั้งข้อมูลที่เป็น Hard copy และ Soft file เอกสาร Hard copy โรงแรมควรมีการจัดเก็บในพื้นที่ที่มีการกำหนดการเข้าถึงว่าบุคคลระดับใดบ้างที่เข้าถึงได้และ อาจมีการล็อกกุญแจ ในส่วนเอกสาร Soft file ซึ่งต้องมีการนำส่งกรมการปกครองผ่านทางเว็บไซต์และอาจมีการเก็บไว้ในฐานข้อมูล โรงแรมควรมีการกำหนดการเข้าถึงของข้อมูล ว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการกำหนดรหัสการเข้าถึงเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

ทั้งนี้ข้อมูลบัตรเครดิตที่เก็บนั้น โรงแรมต้องกำหนดระยะเวลาการทำลายที่ชัดเจนทั้งตัวเอกสาร soft file ที่ผู้เข้าพักมีการส่งให้กับโรงแรมผ่านช่องทางการสื่อสาร หรือกรณีที่โรงแรมมีการพิมพ์เอกสารข้อมูลดังกล่าวออกมาจากระบบ โรงแรมต้องพิจารณาถึงความจำเป็นในการเก็บข้อมูลส่วนนั้น ทั้งข้อมูล Soft file หรือ Hard copy เอกสารกระดาษ อาจกำหนดการทำลายด้วยเครื่องย่อยกระดาษ การเผา หรือการส่งให้บริษัทที่ทำหน้าที่ทำลายเอกสาร ส่วนกรณีเอกสารอิเล็กทรอนิกส์อาจใช้วิธีการลบ หรือทำให้เป็นข้อมูลนิรนามที่ไม่สามารถระบุตัวบุคคลได้

3.2.9 กระบวนการการขายทัวร์ (Tour Desk Process)

การขายทัวร์ หมายถึง การเสนอขายบริการการจัดทำรายการนำเที่ยว (Package tour) ประกอบด้วย การจัดหายานพาหนะ การจัดที่พักค้างคืน การจัดเตรียมเรื่องอาหาร การติดต่อสถานที่ท่องเที่ยว (ธรรมชาติ โบราณสถาน วัฒนธรรม แหล่งบันเทิงเรสซิเดนซ์ต่างๆ) โดยกระบวนการบริหารจัดการขายทัวร์และจัดยานพาหนะ นั้นสามารถแบ่งประเภทการให้บริการได้ออกเป็น 2 กรณี ได้แก่

1. กรณีบริการขายทัวร์ที่ไม่ใช่ของโรงแรม (Outsource tour desk) ซึ่งจะมี 3 รูปแบบย่อย ได้แก่
 - กรณีที่บริษัททัวร์มาเช่าพื้นที่โรงแรมเพื่อขายทัวร์ (Rent space) หมายความว่า บริษัททัวร์ขอเช่าพื้นที่โรงแรมเพื่อขายทัวร์ โดยไม่มีการแลกเปลี่ยนข้อมูลกันระหว่างโรงแรมกับบริษัท

โรงแรมไม่รับรู้ว่ามีขายทัวร์อะไรให้กับใคร จำนวนเท่าไร โปรแกรมไปวันไหน ดังนั้นบริษัททัวร์เป็นผู้ควบคุมข้อมูลแยกออกจากโรงแรม (Separate controller) โดยไม่ต้องมีสัญญาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลระหว่างกัน

- กรณีที่มีการแบ่งเปอร์เซ็นต์ระหว่างโรงแรมกับบริษัททัวร์ (Share commission) หมายความว่า มีการแบ่งปันผลประโยชน์รายได้ระหว่างโรงแรมกับบริษัททัวร์ ซึ่งโดยส่วนมากการชำระเงินก็มักเป็นการ post บิลเข้าห้อง กรณีการแบ่งเปอร์เซ็นต์แบบนี้พนักงานบริษัททัวร์มักสามารถเข้าถึง ข้อมูลของแขกผ่านระบบ โปรแกรมบริหารงานโรงแรม (Hotel Management Software) ได้ ในทางกลับกัน ข้อมูลแขกที่ซื้อทัวร์ไปก็สามารถถูกเข้าถึงได้โดยโรงแรม เพื่อวัตถุประสงค์การแบ่งรายได้ระหว่างกัน ในกระบวนการนี้ ต่างฝ่ายต่างมีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูล ทั้งสองฝ่ายจึงมีสถานะเป็น ผู้ควบคุมข้อมูลแยก (Separate Data Controller) แต่เนื่องจากการแบ่งปันข้อมูลของแขกระหว่างกัน ดังนั้นระหว่าง โรงแรมกับบริษัททัวร์ควรมีการทำสัญญาการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement : DSA) โดยอาจเพิ่มเนื้อหาเข้าไปในสัญญา หรือ แแนบท้ายสัญญา ทั้งนี้ เพื่อช่วยให้คู่สัญญาทราบถึงบทบาทและหน้าที่ของตนเองเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล การกำหนดวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล รวมถึงการกำหนดมาตรฐานในการแบ่งปันข้อมูลส่วนบุคคล สัญญาการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement : DSA) นี้ โรงแรมอาจกำหนดไว้เป็นสัญญาข้อหนึ่ง (Clause) ในสัญญาหลักหรือจัดทำเป็นสัญญาใหม่อีกหนึ่งฉบับ แยกจากสัญญาหลัก หรือจัดทำเป็นข้อตกลงแนบท้าย (Annex) สัญญาพื้นฐานที่มีอยู่เดิมระหว่างโรงแรมและบริษัททัวร์
- กรณีที่บริษัททัวร์จ่ายค่าตอบแทนการขายทัวร์ แบบค่าเช่าพื้นที่และแบ่งเปอร์เซ็นต์โรงแรม (Fixed rent + Share commission) ซึ่งลักษณะและวิธีการจะคล้ายกับข้อกรณีที่มีการแบ่งเปอร์เซ็นต์อย่างเดียว

2. กรณีโรงแรมขายทัวร์เอง (In-house tour desk) ข้อมูลในกรณีกระบวนการนี้มักได้รับการส่งผ่าน (Transit) มาจากลูกค้าตั้งแต่ขั้นตอนกระบวนการลูกค้าแจ้งเข้าและทะเบียนเข้าโรงแรม (Check-in Process) ซึ่งโรงแรมสามารถอ้างอิงฐานสัญญาได้ เพียงแต่โรงแรมต้องมีการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลเพื่อการดำเนินการตามสัญญาให้บริการทัวร์ ให้ผู้เข้าพักซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลทราบด้วย ก่อนหรือขณะที่มีการเก็บข้อมูลส่วนบุคคลทางโรงแรมอาจแจ้งผ่านเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ผู้เข้าพักทราบ ทั้งนี้ ขึ้นอยู่กับความสะดวกของโรงแรม

ข้อมูลที่เก็บนั้น อาจมีการส่งต่อเพื่อทำประกันอุบัติเหตุให้กับผู้เข้าพัก การเปิดเผยดังกล่าวสามารถทำได้เนื่องจาก เป็นหน้าที่ตามกฎหมาย คือ พระราชบัญญัติธุรกิจนำเที่ยวและมัคคุเทศก์ พ.ศ.2551 โรงแรมสามารถใช้ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) ได้

มาตรา ๓๔ ผู้ประกอบธุรกิจจำเป็นต้องจัดให้มีการประกันอุบัติเหตุให้แก่
นักท่องเที่ยว มัคคุเทศก์ และผู้นำเที่ยวในระหว่างเดินทางท่องเที่ยว ทั้งนี้ ตามหลักเกณฑ์ที่
คณะกรรมการประกาศกำหนด

ภาพแสดงหน้าที่ผู้ประกอบธุรกิจต้องจัดทำประกันให้นักท่องเที่ยว
ตาม พระราชบัญญัติธุรกิจนำเที่ยวและมัคคุเทศก์ พ.ศ.2551

โรงแรมต้องมีการกำหนดวิธีในการเก็บรักษา เนื่องจากข้อมูลที่จัดเก็บอาจมีทั้งข้อมูลที่เป็น Hard copy และ Soft file เอกสาร Hard copy โรงแรมควรมีการจัดเก็บในพื้นที่ที่มีการกำหนดการเข้าถึงว่าบุคคลระดับใดบ้างที่เข้าถึงได้และต้องมีการล็อกกุญแจ ในส่วนเอกสาร Soft file ซึ่งอาจมีการเก็บไว้ในฐานข้อมูล โรงแรมควรมีการกำหนดการเข้าถึงของข้อมูล ว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการกำหนดรหัสการเข้าถึง เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

ทั้งนี้ข้อมูลที่เก็บนั้น โรงแรมต้องกำหนดระยะเวลาการทำลายที่ชัดเจนทั้งตัวเอกสาร Soft file ที่ผู้เข้าพักมีการส่งให้กับโรงแรมผ่านช่องทางการสื่อสาร หรือกรณีที่โรงแรมมีการพิมพ์ข้อมูลดังกล่าวออกมาจากระบบ โรงแรมต้องพิจารณาถึงความจำเป็นในการเก็บข้อมูลส่วนนั้น ทั้งข้อมูล Soft file หรือ Hard copy เอกสารกระดาษ อาจกำหนดการทำลายด้วยเครื่องย่อยกระดาษ การเผา หรือการส่งให้บริษัทที่ทำหน้าที่ทำลายเอกสาร ส่วนกรณีเอกสารอิเล็กทรอนิกส์อาจใช้วิธีการลบ หรือทำให้เป็นข้อมูลนิรนาม ที่ไม่สามารถระบุตัวบุคคลได้

3.2.10 กระบวนการ การให้บริการสปา (Spa Service Process)

ในหัวข้อนี้จะกล่าวถึงเฉพาะกรณีที่ผู้เข้าพักใช้บริการในโรงแรมเท่านั้น โดยสปาคือสถานบริการที่ตั้งอยู่ภายในหรือในบริเวณเดียวกันกับโรงแรมหรือรีสอร์ท ที่มีสถานที่ออกกำลังกาย โปรแกรมบริการมักประกอบด้วย การนวดแบบต่าง ๆ ผู้ประกอบการที่มีการเปิดร้านนวดสปาหรือประกอบกิจการธุรกิจสปานั้นจะต้องอยู่ภายใต้ พระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559

ในการเก็บข้อมูลส่วนบุคคลในกระบวนการนี้โดยส่วนใหญ่ กระบวนการสปาอาจมีการเก็บข้อมูลสุขภาพ เพื่อเป็นการคัดกรองและเป็นการป้องกันอันตรายที่อาจเกิดขึ้นกับผู้เข้าพัก เช่น ข้อมูลการแพ้สารเคมี หรือข้อมูลโรคต่าง ๆ ประวัติการผ่าตัด รายละเอียดการบาดเจ็บเกี่ยวกับกระดูก เป็นต้น ข้อมูลสุขภาพนั้น จัดว่าเป็นข้อมูลอ่อนไหว (Sensitive Data) โรงแรมสามารถใช้ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) ว่าด้วยการให้บริการด้านสุขภาพ หรือ การจัดการด้านสุขภาพ ตามมาตรา 24 (5) (ก) ได้ เนื่องจากธุรกิจสปานั้นเป็นธุรกิจที่อยู่ภายใต้ พระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559 โดยกฎหมายกำหนดหน้าที่ให้ผู้ประกอบการมีหน้าที่ต้องสอบถามและบันทึกข้อมูลสุขภาพและคัดกรองผู้รับบริการที่เหมาะสมแก่สุขภาพของผู้รับบริการ พระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559 ตามมาตรา

มาตรา ๓ ในพระราชบัญญัตินี้

“สถานประกอบการเพื่อสุขภาพ” หมายความว่า สถานที่ที่สร้างขึ้นเพื่อดำเนินกิจการ ดังต่อไปนี้

(๑) กิจการสปา อันได้แก่ บริการที่เกี่ยวกับการดูแลและเสริมสร้างสุขภาพโดยวิธีการบำบัดด้วยน้ำ และการนวดร่างกายเป็นหลัก ประกอบกับบริการอื่นตามที่กำหนดในกฎกระทรวงอีกอย่างน้อยสามอย่าง เว้นแต่เป็นการดำเนินการในสถานพยาบาลตามกฎหมายว่าด้วยสถานพยาบาล หรือการอาบน้ำ นวด หรืออบตัวที่เป็นการให้บริการในสถานอาบน้ำ นวด หรืออบตัวตามกฎหมายว่าด้วยสถานบริการ

(๒) กิจการนวดเพื่อสุขภาพหรือเพื่อเสริมความงาม เว้นแต่การนวดเพื่อสุขภาพหรือเพื่อเสริมความงาม ในสถานพยาบาลตามกฎหมายว่าด้วยสถานพยาบาลหรือในหน่วยบริการสาธารณสุขของหน่วยงานของรัฐ หรือการนวดที่เป็นการให้บริการในสถานอาบน้ำ นวด หรืออบตัวตามกฎหมายว่าด้วยสถานบริการ

ความหมายของสถานประกอบการเพื่อสุขภาพ

ตามพระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559

มาตรา ๒๙ ผู้ดำเนินการมีหน้าที่ ดังต่อไปนี้

(๑) จัดทำคู่มือปฏิบัติงานสำหรับบริการหรือคู่มือการใช้อุปกรณ์ ผลิตภัณฑ์และเครื่องมือ เครื่องใช้ต่าง ๆ และพัฒนาผู้ให้บริการให้สามารถให้บริการได้ตามคู่มือที่จัดทำขึ้น

(๒) ควบคุมดูแลการบริการ อุปกรณ์ ผลิตภัณฑ์ และเครื่องมือเครื่องใช้ต่าง ๆ ให้ได้มาตรฐาน ถูกสุขลักษณะ และใช้ได้อย่างปลอดภัย

(๓) สอบถามและบันทึกข้อมูลสุขภาพพื้นฐาน และคัดกรองผู้รับบริการเพื่อจัดบริการที่เหมาะสม แก่สุขภาพของผู้รับบริการ

(๔) ควบคุมดูแลผู้ให้บริการให้ปฏิบัติตามคู่มือการปฏิบัติงานอย่างเคร่งครัด และควบคุมดูแล มิให้ผู้ให้บริการออกไปให้บริการนอกสถานประกอบการเพื่อสุขภาพในเวลางาน

ภาพแสดงหน้าที่ผู้ประกอบการที่ต้องเก็บข้อมูลสุขภาพ

พระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559

ทั้งนี้ ต้องมีการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลให้ผู้ใช้บริการทราบก่อนหรือขณะที่มีการเก็บข้อมูล ส่วนบุคคลทางโรงแรมอาจแจ้งผ่านหน้าเว็บไซต์ ทางอีเมล เอกสาร หรือผ่านทาง QR Code เพื่อให้ นักท่องเที่ยวทราบ ทั้งนี้ขึ้นอยู่กับความสะดวกของโรงแรม

นอกจากนี้โรงแรมต้องมีการกำหนดวิธีในการเก็บรักษา เนื่องจากข้อมูลที่จัดเก็บอาจมีทั้งข้อมูลที่เป็น Hard copy และ Soft file โดยเอกสาร Hard copy โรงแรมควรมีการจัดเก็บในพื้นที่มีการกำหนดการเข้าถึง ว่าบุคคลระดับใดบ้างที่เข้าถึงได้และต้องมีการล็อกกุญแจ ในส่วนเอกสาร Soft file ซึ่งอาจมีการเก็บไว้ใน ฐานข้อมูล โรงแรมควรมีการกำหนดการเข้าถึงของข้อมูล ว่าบุคคลในระดับใดบ้างที่เข้าถึงได้ และควรมีการ กำหนดรหัสการเข้าถึงเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลด้วย

ทั้งนี้ข้อมูลที่เก็บนั้น โรงแรมต้องกำหนดระยะเวลาการทำลายที่ชัดเจนทั้งตัวเอกสาร soft file ที่ผู้เข้าพักมีการส่งให้กับโรงแรมผ่านช่องทางการสื่อสาร หรือกรณีที่โรงแรมมีการพิมพ์ข้อมูลดังกล่าวออกมาจากระบบ โรงแรมต้องพิจารณาถึงความจำเป็นในการเก็บข้อมูลส่วนนั้น ทั้งข้อมูล Soft file หรือ Hard copy เอกสารกระดาษ อาจกำหนดการทำลายด้วยเครื่องย่อยกระดาษ การเผา หรือการส่งให้บริษัทที่ทำหน้าที่ทำลายเอกสาร ส่วนกรณีเอกสารอิเล็กทรอนิกส์อาจใช้วิธีการลบ หรือทำให้เป็นข้อมูลนิรนาม ที่ไม่สามารถระบุตัวบุคคลได้

3.2.11 กระบวนการการทำการตลาดหลัง Check out

เมื่อผู้เข้าพักทำการเช็คเอาท์แล้ว โรงแรมอาจมีการทำการตลาดกับผู้เข้าพักเพื่อวัตถุประสงค์ดังต่อไปนี้ ผู้เข้าพักกลับมาใช้บริการอีกครั้ง เช่น กิจกรรมการเสนอโปรโมชั่นแก่ผู้ที่เคยเข้าพักเป็นหน้าเว็บไซต์หรือแอปพลิเคชัน กิจกรรมการแนะนำสินค้าใกล้เคียงกับที่เคยค้นหา กิจกรรมการส่งอีเมลเฉพาะบุคคล กิจกรรมการสนทนาตอบคำถาม กิจกรรมการเข้าถึงกลุ่มลูกค้าบนโซเชียลมีเดีย กิจกรรมการยิงโฆษณาบนโซเชียลมีเดีย รวมถึงกิจกรรมการยิงโฆษณาเพื่อเข้าถึงกลุ่มบุคคลเดิม (Retargeting) ฯลฯ การใช้หรือส่ง Voucher การให้ราคาพิเศษพร้อมบัตรอวยพรในโอกาสต่าง ๆ เช่น วันเกิด ครบรอบ เป็นต้น

ซึ่งการทำการตลาดกับผู้เข้าพักข้างต้นได้อย่างมีประสิทธิภาพ อาจจะต้องมีการเก็บข้อมูลผู้ใช้งานบนดิจิทัลแพลตฟอร์ม แล้วนำมาวิเคราะห์เพื่อให้สามารถตอบโต้ได้ตรงตามความคาดหวังของแต่ละบุคคล โดยใช้เครื่องมืออัตโนมัติเป็นผู้ช่วย และเนื่องจากการทำการตลาด มีการเก็บรวบรวม วิเคราะห์ และประมวลผลข้อมูลของแต่ละบุคคลเป็นกิจกรรมสำคัญ ดังนั้นโรงแรมจึงควรให้ความสำคัญกับข้อมูลส่วนบุคคลโดยสามารถปฏิบัติตามแนวทางเบื้องต้นดังต่อไปนี้

1) สืบหาข้อมูลส่วนบุคคลที่โรงแรมเป็นเจ้าของ เริ่มต้นด้วยการสำรวจดูว่าข้อมูลส่วนบุคคลของแขกที่มีอยู่นั้นมีที่มาจากช่องทางดิจิทัลใดและอยู่ในรูปแบบใดบ้าง โดยอาจสร้างขึ้นมาเป็น “คลังข้อมูล” หรือ Data Inventory เพื่อจะได้เห็นภาพในองค์กรรวม ซึ่งยิ่งองค์กรใหญ่มากเท่าไรยิ่งอาจมีข้อมูลมากมายมหาศาล มาจากหลากหลายช่องทาง และต้องใช้เวลาในการจัดทำ เมื่อสามารถเห็นช่องทางการเข้ามาของข้อมูลส่วนบุคคลว่ามาจากช่องทางใดบ้าง จัดเก็บไว้ที่ไหน ใครเป็นผู้รับผิดชอบ และมีนโยบายเกี่ยวกับข้อมูลส่วนบุคคลเหล่านั้นเป็นอย่างไร ก็จะสามารถวางแผนจัดการข้อมูลส่วนบุคคลดังกล่าวได้มีประสิทธิภาพในลำดับต่อไป

2) ประเมินวัตถุประสงค์ของการเก็บ ใช้ และเปิดเผยข้อมูล เมื่อเห็นเส้นทางการได้มาของข้อมูลส่วนบุคคลเป็นอย่างไร ก็จะต้องประเมินการนำข้อมูลเหล่านั้นไปใช้เพื่อวัตถุประสงค์ ต้องคำนึงถึงวัตถุประสงค์ที่จริงว่าทำไมจะต้องเก็บข้อมูลเหล่านั้น และมีความต้องการจริง ๆ มากน้อยเพียงใด

โรงแรมต้องระบุวัตถุประสงค์ในการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล อย่างชัดเจนตั้งแต่แรกเมื่อขอความยินยอม “ก่อน” หรือ “ในขณะที่” กำลังเก็บข้อมูลส่วนบุคคล ดังนั้นหากโรงแรมแจ้งวัตถุประสงค์ไปแล้ว และมีการปรับเปลี่ยนใช้ข้อมูลส่วนบุคคลไปในกิจกรรมอื่นที่ไม่สอดคล้องกับวัตถุประสงค์ที่ได้แจ้งถือว่ามี ความผิด (หากไม่ได้ดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคลใหม่อีกครั้งหนึ่ง) การประเมินและทำความเข้าใจ ปริมาณและประเภทของข้อมูลที่โรงแรมต้องการจึงเป็นสิ่งที่ควรกระทำในระยะต้น

3) ชี้แจงต่อเจ้าของข้อมูลส่วนบุคคลอย่างโปร่งใสและเป็นธรรม การดำเนินการให้สอดคล้องกับกฎหมายด้วยการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลอย่างสะอาด โปร่งใส ไม่กำกวม เมื่อบุคคลเหล่านั้นเข้ามาถึงเว็บไซต์หรือแพลตฟอร์มต่าง ๆ ที่เราต้องการเก็บข้อมูลส่วนบุคคล นอกจากเป็นการทำตามกฎหมายแล้ว การชี้แจงแบบนี้ยังเป็นประโยชน์ ช่วยให้เจ้าของข้อมูลรู้สึกไว้วางใจมากขึ้น ซึ่งส่งผลต่อภาพลักษณ์และความสัมพันธ์อันดีต่อแบรนด์และธุรกิจ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ระบุว่าต้องแจ้งขอความยินยอม (Consent) จากบุคคลก่อนหรือระหว่างการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพวกเขา และจะต้องมีลักษณะที่กระทำโดยชัดแจ้ง บ่งบอกถึงวัตถุประสงค์ของการเก็บ ใช้ และเปิดเผยข้อมูลอย่างละเอียด แยกส่วน ออกมาอย่างชัดเจน อ่านง่าย และเข้าใจง่าย โรงแรมจึงควรวางแผนและดำเนินการให้แน่ใจว่าแบบฟอร์มของความยินยอมของโรงแรมมีลักษณะตามที่กฎหมายระบุ

4) สร้างคุณค่าและประสบการณ์ที่ดีผ่านการใช้ข้อมูลส่วนบุคคล : การมอบข้อมูลส่วนบุคคลให้กับธุรกิจหรือนักการตลาดนับเป็นความเชื่อใจจากลูกค้าผู้เป็นเจ้าของข้อมูล เมื่อได้ข้อมูลส่วนบุคคลมาแล้ว ธุรกิจก็ควรตอบแทนความเชื่อใจนั้น ด้วยการนำข้อมูลนั้นมาสร้างคุณค่าและประสบการณ์ที่ดีให้กับลูกค้าอย่างเป็นรูปธรรม จากการสำรวจในระดับโลก พบว่าผู้ตอบคำถาม 79% เต็มใจที่จะแบ่งปันข้อมูลส่วนบุคคลหากเห็นว่า มีประโยชน์กับตนเองอย่างชัดเจน ไม่ว่าจะในรูปแบบของความบันเทิง ข่าวสารสิทธิประโยชน์ หรือรางวัลต่าง ๆ ซึ่งหากโรงแรมสามารถสร้างคุณค่าและมอบประสบการณ์ที่ดีแก่เจ้าของข้อมูลได้อย่างต่อเนื่อง เจ้าของข้อมูลก็มีแนวโน้มที่จะเปิดเผยข้อมูลเพิ่มขึ้น ด้วยหวังว่าโรงแรมจะได้สร้างความประทับใจให้กับพวกเขาได้มากขึ้นอีก

การทำการตลาดโดยตรงไปยังเจ้าของข้อมูลสามารถเติบโตเฟื่องฟูในยุคของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ หากมีการวางแผนศึกษาการไหลเวียนของข้อมูลส่วนบุคคลภายในองค์กร วางวัตถุประสงค์ในการเก็บ ใช้ และเปิดเผยข้อมูล พร้อมทั้งแจ้งให้เจ้าของข้อมูลทราบอย่างละเอียดถี่ถ้วน และนำข้อมูลนั้นมาใช้ประโยชน์อย่างชัดเจน แผนกเข้ากับประเด็นทางเทคนิคที่มีส่วนในการคุ้มครองข้อมูลส่วนบุคคลไม่ให้รั่วไหลหรือถูกทำไปใช้ในทางที่ผิด

3.3 กรณีศึกษา

3.3.1. กรณีศึกษา โรงแรม Marriott ถูกขโมยข้อมูลของผู้เข้าพักผู้เข้าพักกว่าจำนวน 339 ล้านคน

สำนักงานคณะกรรมการข้อมูลข่าวสาร (Information Commissioner Office - ICO) สั่งปรับเครือโรงแรม Marriott เป็นจำนวนเงิน 18.4 ล้านปอนด์ หลังจากข้อมูลของผู้เข้าพักผู้เข้าพักจำนวน 339 ล้านคนถูกขโมยไปจากเครือโรงแรม

เหตุการณ์การถูกละเมิดข้อมูลนั้นเกิดขึ้นในปี 2014 และส่งผลกระทบต่อเครือรีสอร์ท Starwood ที่ Marriott เข้าซื้อกิจการในปี 2015 ด้วย เหตุการณ์เกิดขึ้นจากผู้โจมตีสามารถเข้าถึงระบบของ Starwood และได้ดำเนินการใช้มัลแวร์ผ่านเว็บเซิร์ฟเวอร์ถึงเครื่องมือการเข้าถึงจากระยะไกล เพื่อทำการรวบรวมประวัติและรายละเอียด (credential) ของระบบ จากนั้นผู้โจมตีสามารถเข้าถึงฐานข้อมูลที่ใช้ในการจัดเก็บข้อมูลการจองของผู้เข้าพักรวมถึงชื่อ นามสกุล ที่อยู่, อีเมล, หมายเลขโทรศัพท์, หมายเลขหนังสือเดินทาง, รายละเอียดการเดินทางและข้อมูลโปรแกรม loyalty ของทางโรงแรม ซึ่งการบุกรุกยังคงดำเนินการต่อไปจนถึงปี 2018 โดยที่ทางเครือโรงแรม Marriott ไม่สามารถตรวจพบและตลอดระยะเวลาสี่ปีข้อมูลของผู้เข้าพักผู้เข้าพักประมาณ 339 ล้านคนถูกขโมยไปจากเครือโรงแรม

หน่วยงาน ICO ได้ทำการสอบสวนต่อเหตุการณ์ที่เกิดขึ้นและพบว่าเครือโรงแรม Marriott ได้ทำการฝ่าฝืนข้อกำหนดการป้องกันข้อมูลและการบังคับใช้กฎระเบียบของ (General Data Protection Regulation - GDPR) ที่ออกในปี 2018 ซึ่งด้วยเหตุนี้ ICO สั่งปรับเครือโรงแรม Marriott เป็นจำนวนเงิน 99 ล้านปอนด์ แต่ด้วยสถานะการ COVID-19 ซึ่งทำให้เครือโรงแรม Marriott เกิดสถานะขาดทุนทางการเงิน จึงทำให้เกิดการต่อรองและเจรจาขอลดในส่วนของค่าปรับและเครือโรงแรม Marriott ได้ถูกแก้ไขค่าปรับเป็นเงินจำนวน 18.4 ล้านปอนด์

ทั้งนี้เหตุการณ์การบุกรุกเครือข่ายทางเครือโรงแรม Marriott ได้ทำการปรับปรุงด้านความปลอดภัยทางไซเบอร์เพื่อลดความเสี่ยงต่อความเสียหายที่ลูกค้าได้รับแล้ว

3.3.2. กรณีศึกษา เว็บไซต์รับจองที่พัก Booking.com ถูกปรับเนื่องจากไม่รายงานการละเมิดข้อมูลภายในระยะเวลาที่กำหนด

เว็บไซต์จองการเดินทาง Booking.com ถูกปรับเป็นเงิน 475,000 ยูโร หลังจากไม่รายงานการละเมิดข้อมูลภายในระยะเวลาที่กำหนดโดยกฎหมายคุ้มครองข้อมูลทั่วไป (GDPR)

Booking.com ประสบปัญหาในปี 2018 เมื่อมีฉาชีพได้มีการเจาะเข้าข้อมูลจากทางโทรศัพท์โดยมุ่งเป้าไปที่พนักงาน 40 คนในโรงแรมหลายแห่งในสหรัฐอาหรับเอมิเรตส์ (UAE) หลังจากที่ถูกแฮกเกอร์สามารถเจาะเข้าระบบ Booking.com ทำให้สามารถเข้าถึงข้อมูลส่วนบุคคลของลูกค้ากว่า 4,100 รายที่จองห้องพักโรงแรมในสหรัฐอาหรับเอมิเรตส์ผ่านทางเว็บไซต์ รายละเอียดบัตรเครดิตของลูกค้า 283 รายถูกเปิดเผย และใน 97 รายรหัส CVV ก็ถูกแฮคเช่นเดียวกัน นอกจากนี้ แฮกเกอร์ยังพยายามเข้าถึงรายละเอียดบัตรเครดิตของเหยื่อรายอื่นด้วยการปลอมตัวเป็นพนักงานของ Booking.com ผ่านทางอีเมลหรือทางโทรศัพท์อีกด้วย

Booking.com ซึ่งมีสำนักงานใหญ่ในเนเธอร์แลนด์ได้รับแจ้งการละเมิดเมื่อวันที่ 13 มกราคม 2019 แต่ไม่สามารถรายงานต่อหน่วยงานคุ้มครองข้อมูลของเนเธอร์แลนด์ (AP) จนถึงวันที่ 7 กุมภาพันธ์ (22 วันต่อมา) ซึ่งตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคพื้นยุโรป (GDPR) กำหนดว่าต้องรายงานการละเมิดข้อมูลภายใน 72 ชั่วโมง

ในส่วนของประเทศไทยนั้น ได้มีการกำหนดเรื่องการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ใน มาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่ง ได้กำหนดว่า การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน 72 ชั่วโมง “ นับแต่ทราบเหตุ ” เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

หากกรณีการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ดังนั้นจุดเริ่มต้นสำคัญที่สุดของการเริ่มนับระยะเวลา คือ “ นับแต่ทราบเหตุ ” (become aware)

3.3.3. กรณีศึกษา โรงแรม Accor ถูกปรับ เพราะทำผิดหลักการขอความยินยอม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศสหรือ (CNIL) ได้สั่งปรับ ACCOR SA เป็นจำนวน 600,000 ยูโร ในระหว่างการสืบสวน CNIL พบว่าผู้เข้าพักของโรงแรมที่ทำการจองโดยตรงกับโรงแรมหรือบนเว็บไซต์ได้รับข่าวโฆษณาซึ่งมีลักษณะเป็นการทำการตลาด เนื่องจากช่องยินยอมรับจดหมายข่าวถูกทำเครื่องหมายไว้ล่วงหน้าแล้ว (Pre-ticked) นอกจากนี้ CNIL ยังพบว่าเนื่องจากปัญหาทางเทคนิค ทำให้หลายคนไม่สามารถยกเลิกการรับอีเมลส่งเสริมการขายได้ รวมถึงพบว่า ACCOR ไม่ได้แจ้งให้เจ้าของข้อมูลทราบอย่างเพียงพอเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของตนในบริบทของข้อความส่งเสริมการขาย และด้วยเหตุนี้จึงเป็นการละเมิด มาตรา 12 GDPR และมาตรา 13 GDPR

นอกจากนี้ ACCOR ยังไม่สามารถตอบสนองต่อคำขอของเจ้าของข้อมูลสำหรับการเข้าถึงข้อมูลส่วนบุคคลในเวลาที่กำหนด ไม่ดำเนินการให้เจ้าของข้อมูลสามารถคัดค้านได้ และยังละเมิดมาตรา 32 GDPR เนื่องจาก ACCOR อนุญาตให้ใช้รหัสผ่านที่มีความปลอดภัยไม่เพียงพอ ซึ่งการละเมิดดังกล่าวส่งผลกระทบต่อหลักการพื้นฐานหลายประการของการคุ้มครองข้อมูลส่วนบุคคล และถือเป็นการละเมิดสิทธิ์ขั้นพื้นฐานของเจ้าของข้อมูล

ในการขอความยินยอมนั้น หากเทียบกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฐานความยินยอม (Consent) มาตรา 19 ได้มีการกำหนดว่า ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจาก เจ้าของข้อมูลส่วนบุคคล

- 1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล
- 2) การขอความยินยอมต้องทำโดยชัดแจ้ง แยกส่วนจากข้อความอื่นอย่างชัดเจน
- 3) แจ้งวัตถุประสงค์อย่างชัดเจน

- 4) มีแบบ และข้อความที่ เข้าถึงได้ง่าย และเข้าใจได้
- 5) ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงทำให้เข้าใจผิดในวัตถุประสงค์
- 6) การให้ความยินยอมต้องมีความอิสระ และต้องไม่เป็นส่วนหนึ่งของสัญญา หรือบริการ
- 7) ต้องถอดถอนง่ายเช่นเดียวกับตอนให้ความยินยอม และจะถอนความยินยอมเมื่อใดก็ได้
- 8) หากการถอนความยินยอมมีผลกระทบในเรื่องใด ต้องแจ้งให้เจ้าของข้อมูลทราบ

3.3.4. กรณีศึกษา บริษัท TAXA 4x35 ถูกปรับ เพราะไม่ลบข้อมูลลูกค้าเมื่อสิ้นสุดการใช้งาน

เมื่อวันที่ 21 ธันวาคม ปี 2020 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของเดนมาร์ก (DPA) ได้สั่งปรับ บริษัท TAXA 4x35 ซึ่งเป็นบริษัทที่ให้บริการแท็กซี่ เป็นจำนวนเงินกว่า 180,000 ดอลลาร์ เนื่องจากมีการเก็บข้อมูลหมายเลขโทรศัพท์ ข้อมูลที่อยู่ บริษัทไม่มีการลบทิ้ง ลบเพียงแต่ชื่อ เมื่อผ่านไป 2 ปี แต่อย่างไรก็ตาม ข้อมูลดังกล่าวยังคงสามารถระบุตัวบุคคลได้อยู่ จากการตรวจสอบของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของเดนมาร์ก (DPA) พบว่า มีข้อมูลที่ถูกบันทึกไว้มากถึง 8,000,000 ข้อมูล

เมื่อเทียบกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สิทธิขอให้ลบข้อมูลและสิทธิที่จะถูกลืม ตามมาตรา 33 เจ้าของข้อมูลมีสิทธิขอให้ลบ ทำลาย หรือ ทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีดังนี้

- 1) เมื่อหมดความจำเป็นที่จะเก็บรักษาตามวัตถุประสงค์
- 2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม และผู้ควบคุมข้อมูลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผย
- 3) เมื่อเจ้าของข้อมูลคัดค้าน ตาม ม.32 และ ผู้ควบคุมข้อมูล ไม่สามารถปฏิเสธได้ตามกฎหมาย
- 4) เมื่อเป็นข้อมูลที่เก็บรวบรวม ใช้ หรือเปิดเผย โดยไม่ชอบตามกฎหมาย

4. บทบาทโรงแรมในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

โรงแรมในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือ **Data Controller** กล่าวคือ เป็นบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นผู้ประกอบการที่ทำธุรกิจในนามบุคคลธรรมดา หรือทำในรูปแบบบริษัท และไม่ว่าจะเป็นบริษัทเล็กหรือบริษัทใหญ่ ประกอบกิจการเป็นบริษัทจำกัด หรือ บริษัทมหาชนจำกัด และไม่ได้จำกัดแต่เฉพาะในภาคธุรกิจเท่านั้น หน่วยงานของรัฐก็เช่นกัน หากเขาเหล่านั้น มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เขามีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล”

หน้าที่ของผู้ควบคุมข้อมูล มีดังนี้

หน้าที่	รายละเอียด
1.เก็บรวบรวม ใช้ เปิดเผย ให้เป็นไปตามกฎหมาย	การเก็บรวบรวม ใช้ เปิดเผย ต้องมีฐานทางกฎหมายรองรับ ดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ และต้องดำเนินการเก็บรวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคลเองโดยตรง เว้นแต่เข้าข้อยกเว้น ซึ่งเกี่ยวข้องกับหน้าที่ในการจัดเตรียมเอกสารต่าง ๆ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมั่นใจว่า หากยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลเข้าไปเก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอย่างไร ตัวอย่างเช่น โรงแรมมีหน้าที่ต้องจัดเก็บรวบรวมข้อมูลลูกค้า ได้แก่ ชื่อ นามสกุล วันที่เริ่มจ้าง อัตราค่าจ้าง เพื่อจัดทำทะเบียนลูกค้า ตามกฎหมายคุ้มครองแรงงาน เป็นต้น
2.เปิดช่องให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมาย	บันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เมื่อผู้ควบคุมข้อมูลส่วนบุคคล ปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมระบุเหตุผลในรายการบันทึกการปฏิบัติตามมาตรา 39 ตัวอย่างเช่น พนักงานของโรงแรมขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคล แต่การเข้าถึงดังกล่าวนั้นไปกระทบสิทธิของบุคคลอื่น เช่นนี้โรงแรมมีสิทธิในการปฏิเสธได้ และต้องมีการบันทึกเหตุแห่งการปฏิเสธไว้
3.จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล	เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเป็นไปตามมาตรฐานขั้นต่ำ ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของลูกค้าในโรงแรมว่าในกิจกรรมนั้นๆ ว่าฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือ

หน้าที่	รายละเอียด
	ในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อกกุญแจหรือไม่
4.จัดให้มีมาตรการป้องกันการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ	ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น มีการโอนข้อมูลส่วนบุคคลให้ผู้ประมวลผล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ถูกต้องตามกฎหมาย
5.จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้	จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ตัวอย่างเช่น ข้อมูลทะเบียนลูกจ้าง ควรมีการจัดเก็บอย่างน้อย 2 ปี และควรมีการทำลายเมื่อหมดความจำเป็นในการจัดเก็บ หรือในกรณีที่มีข้อพิพาทระหว่างนายจ้าง หรือลูกจ้าง โรงแรมอาจสามารถเก็บได้ถึง 10 ปี ตามอายุความ กฎหมายแพ่งและพาณิชย์
6.แจ้งเหตุการณั้ละเมิดข้อมูลส่วนบุคคล	ต้องแจ้งเหตุละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับแต่เมื่อทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณั้ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ล่าช้า
7.แต่งตั้งตัวแทนในราชอาณาจักร	หากผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลต้องแต่งตั้งตัวแทนของตนในประเทศไทย โดยต้องแต่งตั้งเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในประเทศไทยและได้รับมอบอำนาจให้กระทำการโดยไม่มีข้อจำกัดความรับผิดชอบใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของผู้ควบคุมข้อมูล
8.หน้าที่ในการจัดทำบันทึกการประมวลผลข้อมูล (Record of	ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการประมวลผลข้อมูล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์

หน้าที่	รายละเอียด
Processing Activities: RoPA)	
9.จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)	การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลและมีมาตรฐานในการดำเนินการภายใต้กรอบของกฎหมาย
10.แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคล (Data Protection Officer: DPO)	หากเข้าหลักเกณฑ์ที่กฎหมายกำหนดให้ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบหากองค์กรเป็นผู้ตัดสินใจจะเก็บรวบรวมข้อมูลส่วนบุคคลของใคร ใช้ข้อมูลอะไร มีวัตถุประสงค์อย่างไร ถือว่าเข้าข่ายเป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่ไม่ได้มีหน้าที่แค่จัดทำประกาศ

5. ขั้นตอนการเตรียมความพร้อมขององค์กร

สิ่งที่โรงแรมต้องเตรียมตัวและปฏิบัติตามกฎหมาย สามารถสรุปได้ทั้งหมด 10 ขั้นตอนดังนี้

1. ผู้บริหารองค์กร ต้องเป็นผู้นำ แสดงบทบาท และให้ความสำคัญกับการบังคับใช้กฎหมายอย่างจริงจัง ผู้บริหารต้องสื่อสารด้วยการปฏิบัติจริง สนับสนุน ส่งเสริม และผลักดันอย่างเป็นรูปธรรม โดย

- ต้องปฏิบัติหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคล ที่ระบุในมาตราต่าง ๆ ตาม กฎหมาย PDPA และกฎหมายที่เกี่ยวข้องอื่น ๆ ที่เกี่ยวข้อง
- กำหนดนโยบาย เพื่อเป็นแนวปฏิบัติที่สอดคล้องกับกฎหมาย ให้กับผู้ที่เกี่ยวข้องในโรงแรม หรือออกข้อบังคับภายในโรงแรม และจัดไว้ในสถานที่ที่เข้าตรวจได้
- แต่งตั้งคณะกรรมการ เพื่อร่วมกันศึกษา PDPA
- สนับสนุนการดำเนินงาน งบประมาณ และทรัพยากรต่าง ๆ ที่จำเป็น
- เข้าร่วมกับคณะกรรมการตามโอกาสสมควร เพื่อคอยชี้แนะ ให้คำปรึกษา ตัดสินใจ หรือส่งเสริม คณะทำงาน เพื่อให้ทำงานได้อย่างราบรื่น และมีประสิทธิภาพ

2. แต่งตั้งคณะกรรมการ โดยผู้บริหารระดับสูง ต้องแต่งตั้งคณะกรรมการพร้อมมอบความรับผิดชอบ และอำนาจหน้าที่ ในการร่วมกันศึกษาข้อกฎหมาย และจัดทำแนวปฏิบัติต่าง ๆ ที่เกี่ยวกับ

3. จัดอบรมคณะกรรมการและผู้บริหารระดับสูง เพื่อให้ผู้บริหารระดับสูง และคณะกรรมการมีความรู้ความเข้าใจเกี่ยวกับกฎหมาย มีความเข้าใจที่ตรงกัน สามารถปฏิบัติหน้าที่ตามที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ

4. วิเคราะห์ ศึกษา ค้นหา และจำแนกรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล ด้วยการทำ Data Inventory Mapping (DIM) ในทุก ๆ กระบวนการของโรงแรม เพื่อรวบรวมว่ามีการเก็บรวบรวม ใช้ หรือเปิดเผย ส่ง/โอน ข้อมูลส่วนบุคคล จากแหล่งใด มีข้อมูลส่วนบุคคลอะไรบ้าง เก็บรวบรวมไว้เพื่อวัตถุประสงค์ใด เก็บมาด้วยวิธี หรือเครื่องมือ หรือช่องทางไหน มีการเปิดเผย หรือส่งไปให้หน่วยงาน หรือบุคคลใด เก็บรักษาข้อมูลไว้ที่แหล่งใดบ้าง มีมาตรการคุ้มครองข้อมูล การกำหนดสิทธิการเข้าถึงอย่างไร มีใครเกี่ยวข้องบ้าง มีการส่ง/โอนไปนอกโรงแรม หรือต่างประเทศหรือไม่ และเมื่อหมดความจำเป็น หรือต้องลบทำลาย มีระยะเวลาจัดเก็บ และวิธีลบทำลายอย่างไร เป็นต้น รวมถึงนำผลที่ได้มาทำการวิเคราะห์การไหลของข้อมูลส่วนบุคคลด้วยการทำ Data Flow Diagram (DFD) เพื่อหาความสัมพันธ์ของข้อมูลส่วนบุคคลกับบุคคล หน่วยงาน หรือองค์กร เพื่อค้นหาจุดเสี่ยง หรือช่องโหว่ ที่จะเกิดการละเมิด หรือรั่วไหลของข้อมูลส่วนบุคคลได้ แล้วนำไปประเมินโอกาส และผลกระทบ (Data Protection Impact Assessment: DPIA) แล้วประเมินความเสี่ยง รวมถึงกำหนดมาตรการตอบสนองกับความเสี่ยงนั้น ๆ

5. จัดทำเอกสารและประกาศใช้ เพื่อแสดงให้เห็นถึงความสอดคล้องกับกฎหมายในการปฏิบัติงาน โรงแรมจำเป็นต้อง สร้างระบบเอกสาร หรือวิธีการที่จำเป็นต่อการปฏิบัติตามกฎหมายขึ้นมา ตัวอย่างเช่น

- นโยบายคุ้มครองความเป็นส่วนตัว (Privacy policy) เพื่อแสดงถึงเจตนารมณ์ในการที่สถานประกอบการจะดำเนินการให้สอดคล้องกับ พรบ. ด้วยการประกาศนโยบายและแนวทางของ

ผู้บริหารระดับสูงในการวางกรอบในการทำงานให้ผู้ได้บังคับบัญชา และผู้ที่เกี่ยวข้องปฏิบัติ ตามกฎหมายการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

- ประกาศความเป็นส่วนตัว (Privacy Notice) เพื่อแสดงให้เห็นว่าโรงแรมได้มีการแจ้ง รายละเอียดต่าง ๆ ให้เจ้าของข้อมูลทราบตามที่กฎหมายกำหนด โดยประกาศความเป็นส่วนตัวจะต้องประกาศในทุกกระบวนการที่เป็นจุด Touch point หรือที่มีปฏิสัมพันธ์กับ เจ้าของข้อมูล
- หนังสือขอความยินยอม (Consent form) ในกรณีที่ไม่ได้รับการยกเว้นตามกฎหมาย สำหรับการประมวลผลที่นอกเหนือจากกฎหมายกำหนด และโรงแรมมีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น การติดต่อสื่อสารเพื่อแจ้งข้อมูลบริการ หรือการ ให้บริการต่าง ๆ จำเป็นต้องมีการขอความยินยอมโดยชัดแจ้ง
- บันทึกการรายการกระบวนการ (Record of Processing Activity: RoPA) เป็นการทำบันทึก รายการประมวลผลตามกฎหมาย
- แบบฟอร์มการใช้สิทธิของเจ้าของข้อมูล (Data Subject Rights Request Form: DSR Form) โรงแรมจำเป็นต้องมีระบบการรองรับการใช้สิทธิของเจ้าของข้อมูล
- การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification) ในกรณีที่เกิด การละเมิดข้อมูลส่วนบุคคล โรงแรมต้องมีการแจ้งรายละเอียดต่างๆที่เกิดขึ้น แก่สำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
- หนังสือข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement: DPA) ในกรณีที่ โรงแรมมีการส่งให้องค์กรอื่น ทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง เพื่อเป็นการ ควบคุมให้องค์กรดังกล่าวซึ่งถือว่าเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ปฏิบัติตามกฎหมาย PDPA จึงจำเป็นต้องมีการทำข้อตกลงระหว่างกัน

6. จัดอบรมและปฐมนิเทศให้กับผู้ที่เกี่ยวข้องทุกระดับ เพื่อให้ระบบ หรือระเบียบปฏิบัติที่กำหนดขึ้น ได้รับการปฏิบัติอย่างถูกต้อง เหมาะสม จำเป็นต้องให้ความรู้กับผู้ที่เกี่ยวข้อง โดยเฉพาะผู้ที่มีหน้าที่ปฏิบัติงาน เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลทราบ โดยหัวข้อ รายละเอียด วิธีการ และระยะเวลาในการอบรมนั้น ขึ้นอยู่กับกลุ่มบุคคล และหน้าที่ที่เกี่ยวข้องนั้น ๆ ไม่จำเป็นต้องอบรมเหมือนกัน ซึ่งต้องมีการวางแผนการอบรม ให้เหมาะสม สอดคล้อง เพื่อให้เกิดประสิทธิภาพ เป็นไปตามวัตถุประสงค์ เกิดความรู้ ความเข้าใจและความ ตระหนักทั่วทั้งองค์กร

7. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยคัดเลือกจากความรู้ ความสามารถ และประสบการณ์ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

8. จัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

9. จัดให้มีการตรวจสอบ และทบทวนความสอดคล้องกับกฎหมาย ได้แก่ กฎหมายลำดับรอง และ กฎหมายที่เกี่ยวข้องอยู่เสมอ

10. ปฏิบัติการในการคุ้มครองข้อมูลส่วนบุคคล และทบทวนแก้ไขอย่างต่อเนื่อง โดยจัดให้มีการตรวจติดตามภายใน หรือให้องค์กรภายนอกทำการตรวจสอบให้เป็นระยะ เพื่อประเมินความสอดคล้อง หากจุดอ่อนของการปฏิบัติ ที่อาจส่งผลให้เกิดความไม่สอดคล้องกับกฎหมาย พร้อมทั้งจัดประชุมทบทวนเป็นระยะตามความเหมาะสม เพื่อทบทวน และทำให้เกิดการปรับปรุงอย่างต่อเนื่อง เป็นการสร้างความมั่นใจ และสร้างความเชื่อมั่น ป้องกันปัญหาที่จะเกิดขึ้นกับโรงแรมในอนาคตได้



ภาคผนวก

1. กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

<https://ratchakitcha.soc.go.th/documents/17082307.pdf>

2. พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566

<https://ratchakitcha.soc.go.th/documents/140A048N0000000004500.pdf>

3. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565

<https://ratchakitcha.soc.go.th/documents/139D140S0000000002400.pdf>

4. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกระบวนการการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

<https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000002600>

5. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

<https://ratchakitcha.soc.go.th/documents/139D140S0000000002800.pdf>

6. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

<https://ratchakitcha.soc.go.th/documents/17233460.pdf>

7. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565

<https://ratchakitcha.soc.go.th/documents/139D140S0000000003200.pdf>

8. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. 2565

http://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/165/T_0001.PDF

9. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2566

<https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf>

10. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

<https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf>

11. พระราชบัญญัติโรงแรม พ.ศ. 2547

<https://ratchakitcha.soc.go.th/documents/150908.pdf>

12. พระราชบัญญัติคนเข้าเมือง พ.ศ. 2522

<https://ratchakitcha.soc.go.th/documents/1421050.pdf>

13. พระราชบัญญัติสถานประกอบการเพื่อสุขภาพ พ.ศ. 2559

<https://ratchakitcha.soc.go.th/documents/2069130.pdf>



PDPA THAILAND

ให้คำปรึกษา พร้อมจัดทำ PDPA & DPO ครบวงจร
โดยทีมผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

เมื่อความไม่รู้ ความไม่เข้าใจ PDPA อย่างแท้จริง
ทำให้เกิดความเสี่ยงที่จะทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ปิดจุดอ่อน แก้ไขข้อผิดพลาด ด้วยบริการของเรา



PDPA&DPO Consultant



ให้คำปรึกษาทางด้านกฎหมาย การบริหารจัดการ
กระบวนการการทำงาน และซอฟต์แวร์ที่เกี่ยวข้อง
กับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Auditor



ตรวจสอบเอกสาร กระบวนการการทำงาน
กระบวนการบริหารจัดการ และเทคโนโลยี
ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Tools



จัดหาเครื่องมือที่จำเป็นในการปฏิบัติตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
เช่น Consent, RoPA, DSRM และ DPIA เป็นต้น

DPO Outsource



ให้บริการเป็น
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือ
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

PDPA&DPO In-House Training



ให้บริการอบรมภายใน ด้วยหลักสูตรบรรยาย
และ Workshop ที่ออกแบบเฉพาะธุรกิจของคุณ
โดยผู้เชี่ยวชาญจากสถาบันพัฒนาและทดสอบ
ทักษะดิจิทัล (DDTI)

PDPA&DPO e-Learning



หลักสูตรออนไลน์ที่ออกแบบเนื้อหา
เกี่ยวกับ PDPA อย่างครบถ้วนและครอบคลุม
ช่วยให้พนักงานเข้าใจ PDPA อย่างง่ายดาย
สะดวก และประหยัดเวลา

บริษัท ดีบีซี กรุ๊ป จำกัด

📍 เลขที่ 125/55 ซอยวิภาวดีรังสิต 60 แขวง 12 เขตจตุจักร กรุงเทพฯ 10210
☎ +66(0)2-029-0707 กด 1-5
📞 +66(0)81-632-5918
✉ pdpa@dbcgroup.asia
📘 PDPA Thailand
📺 PDPA Thailand
🌐 www.dbcgroup.asia



www.pdpathailand.com



@pdpathailand

สนับสนุนโดย

