บริษัท เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน)

นโยบายการคุ้มครองข้อมูลส่วนบุคคล
(Personal Data Protection Policy)

Confidential

Version 1.0, May 2020

S Hotels and Resorts Public Company Limited
123 Suntower Building B, Floor 10th, Vibhavadee Rangsit Road, Chompon, Chatuchak, Bangkok, Thailand 10900

Table of Contents

1. บทนำ 3
2. วัตถุประสงค์ของนโยบาย 3
3. นิยาม 3
4. บทบาท 5
5. ขอบเขตการบังคับใช้นโยบาย 6
6. นโยบายการคุ้มครองข้อมูลส่วนบุคคล 6
   - 6.1 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 6
   - 6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ 7
   - 6.3 สิทธิของเจ้าของข้อมูล 8
   - 6.4 การเก็บรักษาและระยะเวลาในการเก็บรักษาและการทำลายข้อมูลส่วนบุคคล 8
   - 6.5 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล/การจัดการเรื่องร้องเรียน 8
   - 6.6 การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (**Data Protection Impact Assessment: DPIA**) 8
7. การทบทวนนโยบาย 9
8. การละเมิดฝ่าฝืน 9

1. บทนำ

บริษัท เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน) ("บริษัท") ได้จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล ("นโยบาย") ฉบับนี้ เพื่อเป็นมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม และสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ("พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล") และ กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป2016/679 ("GDPR")

2. วัตถุประสงค์ของนโยบาย

- เพื่อเป็นแนวทางในการดำเนินงานต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งรวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงสิทธิของเจ้าของข้อมูล การเก็บรักษาและการทำลายข้อมูลส่วนบุคคล และการจัดการเหตุการละเมิดของข้อมูลส่วนบุคคล
- เพื่อกำหนดขอบเขต อำนาจ หน้าที่ ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน เพื่อเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR

3. นิยาม

ข้อความ หรือ คำใด ๆ ที่ใช้ในนโยบายฉบับนี้ ให้มีความหมายดังต่อไปนี้ เว้นแต่ข้อความดังกล่าวจะแสดงหรือได้อธิบายไว้เป็นอย่างอื่น

คำ หรือ ข้อความ	ความหมาย
บุคคล (Person)	บุคคลธรรมดา
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ข้อมูลส่วนบุคคล: • ข้อมูลแสดงตัวตน (Identity Data): หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ที่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคล ได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล วัน/เดือน/ปีเกิด เพศ เลขบัตรประจำตัวประชาชน หมายเลขใบขับขี่ หมายเลขหนังสือเดินทาง สถานภาพการสมรส เป็นต้น • ข้อมูลติดต่อลูกค้า (Contact Data): เช่น ที่อยู่ อีเมล หมายเลขโทรศัพท์ • ข้อมูลอ่อนไหว (Sensitive Data): คือ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ

	• ข้อมูลทางการเงิน (Financial and Transaction Data): หมายเลขบัญชี หมายเลขบัตรเครดิต และ หมายเลขบัตรเดบิต ข้อมูลรายได้ต่อเดือน ข้อมูลการชำระเงิน เป็นต้น • ข้อมูลทางเทคนิคและการใช้งาน (Technical and Usage data): หมายเลข IP Address ข้อมูลการเข้าสู่ระบบข้อมูลการค้นหา (website browsing) จากการใช้ข้อมูล Cookie ID ประเภทอุปกรณ์การตั้งค่าโปรแกรมและเทคโนโลยีอื่น ๆ ที่ใช้ในการเข้าถึงเว็บไซต์ของบริษัท • ข้อมูลส่วนตัว (Profile Data): ชื่อผู้ใช้และข้อมูลการเข้ารหัส ความสนใจ ความชอบ งบประมาณ เหตุผลในการเลือกซื้อผลิตภัณฑ์และบริการ และข้อมูลความเห็นจากการตอบแบบสำรวจ • ข้อมูลการตลาดและการสื่อสาร (Marketing and Communication data): การตั้งค่าของเจ้าของข้อมูลส่วนบุคคล ในการรับข้อมูลการตลาดจากบริษัทและจากบุคคลที่สาม รวมถึงข้อมูลการติดต่อกับบริษัท เช่น เทปบันทึกกรณีที่ลูกค้าเข้ามาติดต่อทาง Contact Center หรือผ่านทางช่องทาง Social Media อื่น ๆ เป็นต้น • ข้อมูลการจ้างงานและการศึกษา (Employment and Education Data): เช่น หมายเลขประจำตัวพนักงาน ประวัติการจ้างงาน (รวมถึงตำแหน่งงาน ประวัติการทำงาน และประวัติการฝึกอบรม) ประวัติการศึกษา ข้อมูลการรับสมัคร (เช่น CV และจดหมายสมัครงาน) รูปภาพ เงินเดือน และอื่น ๆ ข้อมูลส่วนบุคคลนั้นไม่รวมถึง: • ข้อมูลของผู้ถึงแก่กรรม • ข้อมูลติดต่อทางธุรกิจ เช่น หมายเลขโทรศัพท์ของนิติบุคคล หรือที่อยู่ของนิติบุคคล • ข้อมูลนิรนามหมายถึง ข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
การประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing)	การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม ใช้ เปิดเผย โอน จัดระบบ จัดโครงสร้าง การเก็บรักษา การลบ การเปลี่ยนแปลง การพิจารณา เปิดเผยโดยการส่งต่อ เผยแพร่ ทำให้พร้อมใช้งาน การจัดวาง การผสม การจำกัด การลบหรือทำลาย
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลหรือหน่วยงานของรัฐ ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลใด ๆ ที่ข้อมูลส่วนบุคคลสามารถระบุตัวตนถึงบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ซึ่งหมายรวมถึง พนักงาน ลูกค้า รวมถึงคู่ค้า ผู้ให้บริการ และบุคคลภายนอกอื่นใด

บุคคลที่สาม (Third Party)	บุคคล นิติบุคคล และ/หรือหน่วยงานอื่นที่ บริษัทเปิดเผย รับหรือโอนข้อมูลส่วนบุคคล เช่น ผู้ให้บริการ Outsource บริษัทที่ปรึกษา ผู้รับจ้าง ตัวแทนขาย บริษัททำการตลาด พันธมิตรทางธุรกิจ ตัวแทนจัดหางาน
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Office of the Personal Data Protection Committee)	หน่วยงานของรัฐ ที่รับผิดชอบและกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
เจ้าหน้าที่/คณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer /DPO Working Team : DPO)	เจ้าหน้าที่ หรือคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของบริษัท
คณะกรรมการการคุ้มครองข้อมูลส่วนบุคคลภายใน (DPO Steering Group)	คณะกรรมการการคุ้มครองข้อมูลส่วนบุคคลภายใน ที่ทำหน้าที่เป็นผู้ให้แนวทางการตัดสินใจในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล

4. บทบาท

บริษัท กำหนดโครงสร้างการกำกับดูแลให้การดำเนินงานเป็นไปโดยสอดคล้องกับนโยบายนี้ ดังนี้

หน่วยงาน/บุคลากรผู้ปฏิบัติหน้าที่	หน้าที่ และความรับผิดชอบ
คณะกรรมการการคุ้มครองข้อมูลส่วนบุคคลภายใน (DPO Steering Group)	เป็นผู้ให้แนวทางการตัดสินใจในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล เช่น การให้คำปรึกษาและแนวทางเพื่อแก้ไขปัญหาในประเด็นที่เกิดขึ้นในสายงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล การได้รับเรื่องร้องเรียนจากเจ้าของข้อมูล ได้รับคำร้องขอพิเศษเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นต้น
เจ้าหน้าที่/คณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer /DPO Working Team: DPO)	ให้การสนับสนุนกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบริษัท และ โรงแรม รีสอร์ท ในเครือ ได้แก่ • ให้คำปรึกษา และฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้บุคคลในบริษัท • ตรวจสอบ และติดตามการปฏิบัติตามระเบียบข้อบังคับ

	• เป็นผู้ติดต่อประสานงาน เพื่อให้ความร่วมมือกับหน่วยงานกำกับดูแล ในเรื่องที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล • ตรวจสอบปรับปรุงกระบวนการ และเอกสารที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล • หน้าที่ที่เกี่ยวข้องกับการจัดการเรื่องร้องเรียน • เสนอทบทวนนโยบาย

5. ขอบเขตการบังคับใช้นโยบาย

นโยบายฉบับนี้บังคับใช้กับผู้บริหารและพนักงานทุกหน่วยงานของบริษัท ที่มีการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR รวมถึงใช้กับโรงแรม รีสอร์ท โครงการ และบริษัทร่วมของบริษัท เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน) หากไม่มีนโยบายเรื่องนี้ที่กำหนดเป็นอย่างอื่น

6. นโยบายการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้เป็นไปตามระเบียบ และข้อกำหนดของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลและ GPDR บริษัทกำหนดนโยบาย โดยมีรายละเอียด ดังนี้

6.1 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

6.1.1 บริษัทจะดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ที่ระบุไว้อย่างชัดเจน ทั้งนี้ ในการเก็บรวบรวมและการเปิดเผยในนามของบริษัท จะเป็นข้อมูลที่ถูกต้องและครบถ้วน และไม่ประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้น

6.1.2 บริษัทสามารถดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในกรณีดังต่อไปนี้

- เพื่อเป็นการปฏิบัติตามสัญญา หรือวัตถุประสงค์ที่เห็นพ้องกันระหว่างบริษัท และเจ้าของข้อมูลส่วนบุคคล
- เพื่อเป็นบทบาทหน้าที่ทางกฎหมายของบริษัท หรือเพื่อใช้สิทธิเรียกร้องตามกฎหมาย
- เพื่อเป็นผลประโยชน์อันชอบธรรมของบริษัท เช่น เพื่อการบริหารจัดการภายในรวมถึงการเปิดเผยข้อมูลในกลุ่มธุรกิจเดียวกันเพื่อยกระดับมาตรฐานในการทำงาน หรือเพื่อการรักษาความปลอดภัย และป้องกันการกระทำที่ผิดกฎหมาย
- เพื่อการปฏิบัติหน้าที่ของบริษัทในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ตามที่รัฐได้มอบหมายให้แก่บริษัท
- เมื่อบริษัท ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กรณีที่ได้รับยกเว้นไม่ต้องขอความยินยอมภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR หรือกฎหมายอื่น

6.1.3 บริษัท จะดำเนินการอย่างใดอย่างหนึ่งตามความเหมาะสม เพื่อให้เจ้าของข้อมูลให้ความยินยอม (Consent) และ/หรือรับทราบถึงการเข้าถึงความเป็นส่วนตัว ผ่าน "ประกาศความเป็นส่วนตัว" (Privacy Notice) ซึ่งระบุถึงวัตถุประสงค์ทั้งหมดที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สำหรับวัตถุประสงค์ที่ไม่ถูกระบุในประกาศความเป็นส่วนตัวของบริษัท จะต้องได้รับความยินยอมจากเจ้าของข้อมูลในการประมวลผลเพื่อ

วัตถุประสงค์ดังกล่าวก่อนทุกกรณี (เว้นแต่กรณีที่ได้รับยกเว้นไม่ต้องขอความยินยอมภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล GDPR หรือกฎหมายอื่น) ทั้งนี้ การให้หรือไม่ให้ความยินยอมจะไม่เป็นเงื่อนไขในการรับบริการหรือซื้อผลิตภัณฑ์ของบริษัท

6.1.4 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ เงื่อนไขและข้อกำหนดในการขอความยินยอมจากผู้เยาว์นั้น บริษัท จะดำเนินการให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR

6.1.5 การเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สาม บริษัท จะจัดให้มีข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับผู้ประมวลผลข้อมูลส่วนบุคคลในนามของบริษัท เพื่อกำหนดขอบเขตและหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล และหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลให้เพียงพอตามนโยบายฉบับนี้ เพื่อให้มั่นใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อตกลงกับบริษัท หากมีการละเมิดการใช้ข้อมูลส่วนบุคคลใด ๆ ที่ไม่เป็นไปตามข้อตกลง

6.1.6 ในกรณีที่บริษัทได้รับข้อมูลส่วนบุคคลมาจากแหล่งอื่น เช่น จากบุคคลที่สาม บริษัทจะดำเนินการให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR

6.1.7 ในกรณีที่บริษัทได้รับการร้องขอจากบุคคลที่สามให้ทำการยืนยันว่าบริษัทได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมายังบุคคลที่สาม หน่วยงานที่ได้รับแจ้งการร้องขอจะต้องแจ้งฝ่ายกฎหมายของบริษัทและDPO เพื่อให้ตรวจสอบว่าขอบเขตของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สามมีความสอดคล้องกับข้อกำหนดของนโยบายนี้

6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

บริษัทจะไม่โอนข้อมูลส่วนบุคคลออกนอกราชอาณาจักรไทย เว้นแต่ข้อมูลส่วนบุคคลที่ถูกโอนไปยังประเทศปลายทางนั้นได้รับการคุ้มครองภายใต้มาตรฐานเดียวกัน และ/หรือ

- เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอม โดยบริษัทจะแจ้งให้เจ้าของข้อมูลทราบถึงมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางที่รับข้อมูล
- เป็นการทำเพื่อปฏิบัติตามสัญญาระหว่างบริษัทและเจ้าของข้อมูลส่วนบุคคล หรือเป็นข้อกำหนดในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
- เป็นการกระทำตามสัญญาระหว่างบริษัทกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- ข้อมูลส่วนบุคคลที่ถูกส่งผ่านเครื่องแม่ข่าย (Server) ที่อยู่ในต่างประเทศ ทั้งนี้ ต้องเป็นการกระทำตามสัญญาระหว่างบริษัท กับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- เพื่อปฏิบัติตามกฎหมาย
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- กรณีจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ
- ในกรณีที่บริษัทมีความจำเป็นที่จะต้องโอนข้อมูลไปยังเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ เพื่อประกอบกิจการหรือธุรกิจร่วมกัน บริษัทจะทำการโอนข้อมูลดังกล่าวภายใต้นโยบายการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลในเครือกิจการซึ่งอยู่ต่างประเทศ (Binding Corporate Rules) นโยบายดังกล่าวจะต้องได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่ บริษัท มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของลูกค้าไปต่างประเทศ บริษัทจะจัดทำสัญญา

การคุ้มครองข้อมูลส่วนบุคคลกับคู่สัญญาในประเทศดังกล่าว

6.3 สิทธิของเจ้าของข้อมูล

บริษัทสนับสนุนให้เจ้าของข้อมูลส่วนบุคคลที่มีความประสงค์จะร้องขอให้บริษัทดำเนินการตามสิทธิต่าง ๆ ที่ระบุไว้ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR อย่างชัดเจน ทั้งนี้ บริษัท ได้ระบุสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้ตามรายละเอียดใน "ประกาศความเป็นส่วนตัว"

6.4 การเก็บรักษาและระยะเวลาในการเก็บรักษาและการทำลายข้อมูลส่วนบุคคล

6.4.1 บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ในระยะเวลาเท่าที่จำเป็นในการบรรลุวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล และสอดคล้องกับกฎหมาย เมื่อความสัมพันธ์ทางธุรกิจของบริษัทกับเจ้าของข้อมูลส่วนบุคคลสิ้นสุดลง หรือการเก็บรักษาข้อมูลส่วนบุคคลนั้น ไม่มีความจำเป็นเพื่อวัตถุประสงค์ทางกฎหมายและเพื่อทางธุรกิจอีกต่อไป บริษัทจะพิจารณาเพื่อเก็บรักษาข้อมูล หรือทำลายข้อมูลอย่างเหมาะสม ตามแนวปฏิบัติเกี่ยวกับการเก็บรักษาและการทำลายข้อมูลส่วนบุคคลของบริษัท

6.4.2 บริษัทจะดูแลให้มีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลที่เหมาะสม รวมถึงมีการรักษาความลับของลูกค้า

6.4.3 พนักงานทุกคนของบริษัทมีหน้าที่และความรับผิดชอบ ในการทำให้มั่นใจว่าเอกสารที่มีข้อมูลส่วนบุคคลอยู่นั้น มีการเก็บรักษา รวมถึงถูกทำลายด้วยวิธีการที่เหมาะสม ซึ่งเป็นไปตามแนวปฏิบัติเกี่ยวกับการเก็บรักษาและการทำลายข้อมูลส่วนบุคคลของบริษัท

6.5 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล/การจัดการเรื่องร้องเรียน

6.5.1 เจ้าของข้อมูลส่วนบุคคล และบุคคลที่พบเจอเหตุการณ์เกี่ยวกับการละเมิดข้อมูลส่วนบุคคล สามารถแจ้งการร้องเรียนผ่านช่องทางที่บริษัทกำหนด

E-mail: contactus@shotelsresorts.com

6.5.2 ข้อร้องเรียนทั้งหมดจะถูกส่งต่อไปยัง DPO เพื่อบันทึกการร้องเรียนเกี่ยวกับเหตุการณ์การละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคลทั้งหมดจากทุกช่องทางการร้องเรียน และเก็บเป็นความลับ

6.5.3 หากพบว่ามีผลกระทบต่อสิทธิ เสรีภาพของบุคคลหรืออาจส่งผลกระทบต่อ ชื่อเสียงและความเสียหายทางการเงินต่อบริษัท ให้ DPO ดำเนินการดังนี้

- แจ้งเหตุไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน เพื่อประเมินความเสี่ยงและตัดสินใจในเหตุการณ์การละเมิดดังกล่าว ว่ามีความจำเป็นจะต้องแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลหรือไม่
- หากพบว่ามีความจำเป็น DPO จะต้องรายงานไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับจากที่ทราบเหตุ

6.5.4 หากพบว่าเหตุการณ์การละเมิด มีความเสี่ยงสูงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลให้ทำการแจ้งเหตุการณ์ละเมิดพร้อมทั้งแนวทางเยียวยาไปยังเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า

6.6 การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

บริษัทจะต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง เพื่อเป็นการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และ GDPR

7. การทบทวนนโยบาย

บริษัทต้องทบทวน และปรับปรุงนโยบายอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

8. การละเมิดฝ่าฝืน

การไม่ปฏิบัติตามนโยบาย โดยมิได้รับการยกเว้นตามระเบียบของบริษัท ถือเป็นการฝ่าฝืน ซึ่งมีบทลงโทษทางวินัย ตั้งแต่การตักเตือน คาดโทษ พักงาน เลิกจ้าง และอาจมีการดำเนินคดีทางกฎหมายได้

ประกาศเมื่อ 15 พฤษภาคม 2563

.....

(นายสมพงษ์ ตัณฑพาทย์)

ประธานคณะกรรมการ

บริษัท เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน)