ประกาศ

ที่ DPO 006/2567

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy)

---

1. หลักการและเหตุผล

ด้วยความก้าวหน้าของเทคโนโลยีสารสนเทศ รวมทั้งระบบสื่อสารได้พัฒนาไปอย่างรวดเร็ว ทำให้การเข้าถึง การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล สามารถทำได้โดยง่าย สะดวก และรวดเร็ว อันอาจนำมาซึ่งความเสียหายต่อเจ้าของข้อมูล ประกอบกับได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 แล้วนั้น

บริษัทได้ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัว (Privacy Right) ที่ต้องได้รับความคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย และหลักปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) ซึ่งบุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมาย ต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น รวมถึงเพื่อสนับสนุนและเคารพการปกป้อง สิทธิมนุษยชนตามที่ประกาศใช้ในระดับสากล ตามหลักการของข้อตกลงโลกแห่งสหประชาชาติ (UN Global Compact) รวมถึงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทจึงได้ประกาศนโยบายเพื่อเป็นหลักในการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ดังนี้

2. วัตถุประสงค์

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ จัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

2.1 เพื่อคุ้มครองข้อมูลส่วนของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นบุคคลธรรมดาซึ่งทำธุรกรรม ใช้บริการ มีส่วนได้เสีย หรือที่มีส่วนเกี่ยวข้องกับบริษัท ได้แก่ บุคคลดังต่อไปนี้

ก. ลูกค้า

ข. พนักงาน และผู้สมัครงาน

ค. ผู้ถือหุ้น นักลงทุน

ง. เจ้าหนี้ ลูกหนี้

จ. คู่ค้า พันธมิตรทางธุรกิจ

ฉ. บุคคลที่บริษัทได้ว่าจ้างให้ดำเนินงานตามวัตถุประสงค์ของบริษัท เช่น ที่ปรึกษาด้านวิชาชีพ ผู้ให้บริการด้านระบบเทคโนโลยีสารสนเทศ เป็นต้น

ช. บุคคลที่เข้าชมเว็บไซต์หรือแอปพลิเคชันของบริษัท

ซ. บุคคลที่เข้ามาติดต่อหรือใช้บริการสำนักงาน อาคารหรือสถานที่ของบริษัท

ฌ. ครอบครัวพนักงาน ผู้รับผลประโยชน์ตามกรมธรรม์ประกันชีวิต ประกันวินาศภัยที่บริษัทได้จัดทำให้

ญ. บุคคลที่ถูกอ้างอิง เช่น บุคคลที่ถูกอ้างอิงในการสมัครงาน การเสนอขายสินค้าและบริการกับบริษัท เป็นต้น

2.2 เพื่อกำหนดบทบาทหน้าที่ของหน่วยงาน ผู้บริหาร พนักงาน ซึ่งมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล

2.3 เพื่อกำหนดขั้นตอนหรือมาตรการรักษาความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคล

2.4 เพื่อกำหนดแนวทางในการปฏิบัติงานของพนักงานซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล

2.5 เพื่อสร้างความเชื่อมั่นในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ต่อเจ้าของข้อมูลส่วนบุคคล

3. ขอบเขตการใช้

3.1 ให้ยกเลิกประกาศที่ DPO 004/2566 เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) และใช้ประกาศฉบับนี้แทน

3.2 ให้ประกาศฉบับนี้ มีผลใช้บังคับกับคณะกรรมการ กรรมการ ผู้บริหาร และพนักงานทุกระดับของบริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย (ยกเว้นบริษัท ซีพี แอ็กซ์ตร้า จำกัด (มหาชน) และบริษัทย่อย) รวมถึงคู่ค้า พันธมิตรทางธุรกิจ (Store business partner) ผู้ให้บริการ และผู้มีส่วนได้ส่วนเสียกับบริษัท โดยใช้บังคับกับทุกกิจกรรมการดำเนินงานของบริษัทที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

4. คำนิยาม

"บริษัท"	หมายความถึง บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย
"บริษัทย่อย"	หมายความถึง บริษัทจำกัด หรือบริษัทมหาชนจำกัด ซึ่งอยู่ภายใต้การควบคุมของบริษัท โดยมีลักษณะเป็นไปตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
"ข้อมูลส่วนบุคคล"	หมายความถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม
"ข้อมูลส่วนบุคคลที่มีความอ่อนไหว"	หมายความถึง ข้อมูลส่วนบุคคลที่มีความเสี่ยงอาจถูกนำไปสู่การเลือกปฏิบัติอย่างไม่เป็นธรรม (Sensitive Data) ในที่นี้หมายถึง เชื้อชาติ ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรืออื่น ๆ ตามที่กฎหมายกำหนด
"การประมวลผลข้อมูลส่วนบุคคล"	หมายความถึง การเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล โดยรวมไปถึงการดำเนินการหรือการดำเนินการซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ก็ตาม
"เจ้าของข้อมูลส่วนบุคคล"	หมายความถึง บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล เป็นต้นว่า ลูกค้า คู่ค้า ผู้ใช้บริการ และพนักงาน
"ผู้ควบคุมข้อมูลส่วนบุคคล"	หมายความถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในที่นี้หมายถึง บริษัท หน่วยงาน พนักงานที่รับผิดชอบในข้อมูลส่วนบุคคลนั้น

"ผู้ประมวลผลข้อมูลส่วนบุคคล"	หมายความถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ในที่นี้หมายถึง คู่ค้า บุคคลหรือบริษัทภายนอกที่บริษัทได้ว่าจ้าง
"บุคคล"	หมายความถึง บุคคลธรรมดา
"บุคคลผู้หย่อนความสามารถ"	หมายความถึง บุคคลซึ่งเป็นผู้เยาว์ เป็นคนไร้ความสามารถ หรือเสมือนไร้ความสามารถตามประมวลกฎหมายแพ่งและพาณิชย์
"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" (Data Protection Officer: DPO)	หมายความถึง บุคคลซึ่งบริษัทแต่งตั้งให้ทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ผู้ประสานงานข้อมูลส่วนบุคคล (Data Protection Coordinator: DPC)	หมายความถึง ผู้บริหารสูงสุดของบริษัทย่อย หรือ ผู้บริหารสูงสุดของสำนักในระดับสำนัก หรือเทียบเท่า มีหน้าที่เป็นผู้ประสานงานข้อมูลส่วนบุคคล
"กฎหมายคุ้มครองข้อมูลส่วนบุคคล" (Personal Data Protection Law)	หมายความถึง กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่บริษัทดำเนินกิจการอยู่ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น
"สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล / สคส." (Office of the Personal Data Protection Commission)	หมายความถึง หน่วยงานของรัฐตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีหน้าที่กำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

5. การคุ้มครองข้อมูลส่วนบุคคล

5.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลให้กระทำได้ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายและเท่าที่จำเป็นตามกรอบวัตถุประสงค์หรือเพื่อประโยชน์ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ในการเก็บรวบรวม

5.1.1 แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวม ถึงรายละเอียดดังต่อไปนี้

ก) วัตถุประสงค์และฐานกฎหมายของการเก็บรวบรวม

ข) ระยะเวลาในการเก็บรวบรวมไว้

ค) ประเภทของบุคคล หน่วยงาน ชื่อประเทศซึ่งอาจมีการเปิดเผยข้อมูลส่วนบุคคล

ง) แหล่งที่มาของข้อมูลส่วนบุคคลจากแหล่งอื่น (ถ้ามี)

จ) ข้อมูลหรือช่องทางการติดต่อกับบริษัท และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ฉ) สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการร้องเรียนไปยังสคส.

ช) แจ้งผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่ให้ข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด หรือเพื่อเข้าทำหรือปฏิบัติตามสัญญา

5.1.2 การประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามฐานทางกฎหมายดังต่อไปนี้

ก) เพื่อประโยชน์สาธารณะ การศึกษาวิจัย การสถิติ หรือการปฏิบัติตามกฎหมาย

ข) เป็นการดำเนินการเพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล

ค) เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

ง) เป็นการจำเป็นตามหน้าที่ในการดำเนินการเพื่อประโยชน์สาธารณะ หรือการปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบหมาย

จ) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งประโยชน์โดยชอบด้วยกฎหมายนั้นมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

ฉ) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ช) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และต้องทำโดยชัดแจ้ง มีความเป็นอิสระ ทำเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์

5.1.3 กรณีที่มีการเปลี่ยนแปลงวัตถุประสงค์ ต้องแจ้งวัตถุประสงค์ใหม่ให้แก่เจ้าของข้อมูลส่วนบุคคลทราบและ/หรือได้รับความยินยอมก่อนการประมวลผลข้อมูลส่วนบุคคล

5.2 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

ห้ามเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ได้ดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

5.3 การเก็บรวบรวมข้อมูลส่วนบุคคลของผู้หย่อนความสามารถ

การเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ เพื่อดำเนินการตามวัตถุประสงค์ใด ๆ ซึ่งผู้เยาว์ไม่อาจดำเนินการเองได้โดยลำพังตามที่ประมวลกฎหมายแพ่งและพาณิชย์กำหนดไว้ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองหรือผู้ทำการแทนผู้เยาว์ด้วย เว้นแต่กรณีผู้เยาว์อายุไม่เกิน 10 ปี ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง หรือผู้การแทนผู้เยาว์เท่านั้น

การเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นบุคคลไร้ความสามารถ หรือเสมือนไร้ความสามารถ ต้องได้รับความยินยอมจากผู้อนุบาล หรือจากผู้พิทักษ์ หรือบุคคลผู้ทำการแทนเท่านั้น

5.4 การเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)

บริษัทจะไม่เก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เว้นแต่มีความจำเป็นต้องเก็บรวบรวม โดยต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ในกรณีที่กฎหมายกำหนดให้สามารถเก็บรวบรวมได้โดยไม่ต้องขอความยินยอม

5.5 การใช้และ/หรือการเปิดเผยข้อมูลส่วนบุคคล

การใช้และ/หรือการเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามวัตถุประสงค์ที่ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะทำการเก็บรวบรวม หรือเป็นการจำเป็นเพื่อประโยชน์ที่มีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กรณีที่กฎหมายกำหนดให้ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการปฏิบัติตามกฎหมาย

บุคคลหรือนิติบุคคลอื่น ซึ่งได้รับข้อมูลส่วนบุคคลจากการที่เจ้าของข้อมูลส่วนบุคคลตกลงยินยอมให้เปิดเผยหรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ต้องใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ซึ่งเจ้าของข้อมูลส่วนบุคคลได้ตกลงยินยอมให้ไว้กับบริษัท และตามที่บุคคล หรือนิติบุคคลนั้นได้แจ้งไว้กับบริษัทเท่านั้น

5.6 การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

การส่งหรือโอนข้อมูลส่วนบุคคลทั้งข้อมูลทางกายภาพหรือผ่านระบบคอมพิวเตอร์หรือระบบเครือข่ายให้แก่ผู้รับข้อมูลส่วนบุคคล แต่มิได้หมายรวมถึงการส่งและการรับข้อมูลส่วนบุคคลลักษณะที่เป็นสื่อกลางในการส่งผ่าน (in transit) หรือเก็บข้อมูลเครือข่าย (cloud data storage) หรือการใช้งานบนผู้ให้บริการบนคลาวด์ที่ไม่มีบุคคลอื่นสามารถเข้าถึงได้นอกจากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคลากร พนักงาน หรือลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลส่วนบุคคลนั้น

กรณีที่บริษัทต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทาง ต้องพิจารณาดังต่อไปนี้

5.6.1 สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้ ถ้าประเทศปลายทางมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามที่กฎหมายประกาศ เว้นแต่

- การส่งหรือโอนข้อมูลส่วนบุคคลเป็นการปฏิบัติตามกฎหมาย
- ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ 'ไม่เพียงพอ' ของประเทศปลายทาง
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญา
- ทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น
- เพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

5.6.2 กรณีที่มีการส่งข้อมูลในเครือกิจการเดียวกันที่อยู่ต่างประเทศ ต้องจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการเดียวกัน (Binding Corporate Rule) และต้องได้รับการอนุมัติจากสคส.

5.6.3 จัดทำสัญญาระหว่างผู้โอนกับผู้รับโอนที่อยู่นอกประเทศไทย (Standard Contractual Clauses) โดยใช้แบบฟอร์มสัญญาต้นแบบ หรือข้อความตามที่สคส.ประกาศกำหนด

5.6.4 บริษัทได้รับการรับรอง (Certificate) ในส่วนที่เกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทาง โดยเป็นมาตรฐานที่ สคส.ประกาศ

6. คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้นั้น ต้องถูกต้องเป็นปัจจุบัน สมบูรณ์ ไม่ก่อให้เกิดความเข้าใจผิด และต้องดำเนินการจัดให้มีช่องทางให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอหรือแก้ไขข้อมูลส่วนบุคคลของตัวเองได้

7. ระยะเวลาการเก็บและการลบข้อมูลส่วนบุคคล

บริษัทจะต้องกำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลตามวัตถุประสงค์เท่าที่จำเป็น และเมื่อหมดความจำเป็นตามวัตถุประสงค์จะต้องลบ ทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ (ข้อมูลนิรนาม)

8. บทบาทหน้าที่และความรับผิดชอบ

บริษัทกำหนดให้พนักงานหรือหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องให้ความสำคัญ และรับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

อย่างเคร่งครัด โดยกำหนดให้บุคคลหรือหน่วยงานดังต่อไปนี้ ทำหน้าที่กำกับ และตรวจสอบให้การดำเนินงานของบริษัทนั้นถูกต้อง และเป็นไปตามนโยบาย และกฎหมายคุ้มครองข้อมูลส่วนบุคคล

8.1 ผู้ควบคุมข้อมูลส่วนบุคคล

8.1.1 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ตามระดับความเสี่ยงที่อาจจะเกิดขึ้น และทบทวนมาตรการอย่าง สม่ำเสมอเพื่อให้มาตรการดังกล่าวมีประสิทธิภาพ ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไป

8.1.2 กำหนดขอบเขตการจัดการกับข้อมูลส่วนบุคคลที่ได้เปิดเผยต่อบุคคล หรือนิติบุคคลอื่น

8.1.3 จัดให้มีระบบตรวจสอบการจัดการกับข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายกำหนด

8.1.4 บันทึกรายการเกี่ยวกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

8.1.5 จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล นิติบุคคลหรือบุคคลภายนอกอื่นใด หากมีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้ว่าจ้างนิติบุคคล หรือบุคคลภายนอกอื่นใด โดยผู้ประมวลผลข้อมูล ส่วนบุคคลดังกล่าว ต้องมีมาตรการรักษาความปลอดภัยในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามนโยบายฉบับนี้ และตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

8.2 ผู้ประมวลผลข้อมูลส่วนบุคคล

8.2.1 ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล

8.2.2 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ตามระดับความเสี่ยงที่อาจจะเกิดขึ้น

8.2.3 จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้

8.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

8.3.1 จัดทำและทบทวนนโยบายคุ้มครองข้อมูลส่วนบุคคล รวมถึงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วนและถูกต้องตามที่กฎหมายกำหนด

8.3.2 ให้คำแนะนำในด้านต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้บริหาร พนักงาน และคู่ค้าของบริษัท

8.3.3 ตรวจตราการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

8.3.4 กำกับดูแลหน่วยงานต่าง ๆ ของบริษัท บริษัทย่อย และคู่ค้าของบริษัทให้ดำเนินงานตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

8.3.5 รายงานการปฏิบัติงานหน่วยงานต่าง ๆ ของบริษัท บริษัทย่อย และคู่ค้าของบริษัทต่อคณะเจ้าหน้าที่บริหาร

8.3.6 ประสาน จัดการเรื่องร้องเรียน หรือการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ได้รับการติดต่อ หรือร้องขอจากเจ้าของข้อมูลส่วนบุคคล

8.3.7 ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบริษัท บริษัทย่อย และคู่ค้าของบริษัท

8.3.8 แจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถทำได้

8.3.9 จัดประชุมคณะทำงานคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ

8.4 สำนักกฎหมาย กลุ่มธุรกิจฯ

8.4.1 ให้คำปรึกษา แนะนำ และให้ความเห็นเกี่ยวกับการดำเนินงานให้ถูกต้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

8.4.2 ตรวจสอบ/จัดทำเอกสาร สัญญาที่เกี่ยวข้องให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

8.5 หน่วยงาน Risk Management

8.5.1 ค้นหา และระบุความเสี่ยงในกิจกรรมหรือการดำเนินงานของหน่วยงานต่าง ๆ ของบริษัทที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล

8.5.2 ประเมินความเสี่ยงโดยการกำหนดระดับความเสี่ยงของแต่ละกิจกรรม หรือการดำเนินงาน และระบุความเสี่ยงที่ยอมรับได้ (Risk Appetite)

8.5.3 ติดตามให้แต่ละหน่วยงานดำเนินงานให้อยู่ในความเสี่ยงที่ยอมรับได้ (Risk Appetite)

8.5.4 ทบทวนระดับความเสี่ยงของกิจกรรม หรือการดำเนินงานของแต่ละหน่วยงานทุกไตรมาส

8.5.5 จัดทำรายงาน และมีการรายงานต่อคณะกรรมการบริหาร (Executive Committee)

8.6 ผู้ตรวจสอบภายใน / ผู้ตรวจสอบภายนอก

8.6.1 ตรวจสอบการทำงานของผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

8.6.2 จัดให้มีการตรวจสอบกระบวนการดำเนินงาน เอกสารที่เกี่ยวข้อง และประเมินประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยผู้ตรวจสอบภายใน / ผู้ตรวจสอบภายนอกเป็นประจำทุกปี

8.6.3 รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบของบริษัท

8.7 ผู้บริหารบริษัทย่อย หน่วยงานระดับสำนัก หรือเทียบเท่า (Data Protection Coordinator: DPC)

8.7.1 ให้ผู้บริหารสูงสุดของบริษัทย่อย หรือผู้บริหารสูงสุดของสำนักในระดับสำนัก หรือเทียบเท่า มีหน้าที่สั่งการ ควบคุม กำกับดูแลให้พนักงานภายในสังกัดของตนปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายฉบับนี้โดยเคร่งครัด โดยให้มีหน้าที่เป็นผู้ประสานงานข้อมูลส่วนบุคคล (Data Protection Coordinator: DPC) รวมถึงการจัดการความเสี่ยง และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งเกิดขึ้นในบริษัทหรือหน่วยงานของตนต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

8.7.2 ผู้บริหารบริษัทย่อย หน่วยงานระดับสายงานหรือระดับสำนักหรือเทียบเท่า สามารถออกข้อกำหนดหรือระเบียบปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้บังคับภายในหน่วยงานของตนได้ ทั้งนี้ ข้อกำหนดหรือระเบียบปฏิบัติดังกล่าวนั้น ต้องเป็นไปตามนโยบายฉบับนี้ และตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และต้องแจ้งให้กับสำนักกฎหมายกลุ่มธุรกิจฯ ทราบ

9. การรักษาความมั่นคงปลอดภัย

โดยบริษัทกำหนดให้บุคลากรของบริษัท และผู้รับจ้างภายนอกจะต้องปฏิบัติตามมาตรการดังต่อไปนี้อย่างเคร่งครัดเพื่อประโยชน์ในการรักษาความลับ และความปลอดภัยของข้อมูลส่วนบุคคล

9.1 กำหนดการบริหารจัดการการเข้าถึงข้อมูลส่วนบุคคล (Access Control) รวมถึงการแสดงหรือยืนยันตัวบุคคล ผู้เข้าถึงหรือใช้ข้อมูลส่วนบุคคล (Authentication) จัดให้มีมาตรการรักษาความปลอดภัย รวมถึงกระบวนการทบทวน และประเมินประสิทธิภาพของมาตรการรักษาความปลอดภัยดังกล่าว ทั้งนี้ เป็นไปตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยี

สารสนเทศ (Information Technology Security Policy) และนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ของบริษัทอย่างเคร่งครัด

9.2 ในการส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บบนฐานข้อมูลในระบบอื่นใด ซึ่งผู้ให้บริการรับโอนข้อมูล หรือบริการเก็บรักษาข้อมูลอยู่ต่างประเทศ ประเทศปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่า หรือดีกว่ามาตรการตามนโยบายนี้

9.3 ในกรณีที่มีการฝ่าฝืนมาตรการการรักษาความมั่นคงปลอดภัยของบริษัท จนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล บริษัทจะดำเนินการตามนโยบายการละเมิด และข้อมูลรั่วไหล (Data Breach Handling Policy) และตามที่กฎหมายกำหนด หากการละเมิดนั้นมีความเสี่ยงที่จะกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล บริษัทจะดำเนินการแจ้งเหตุการละเมิดพร้อมทั้งแนวทางการเยียวยาให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า ทั้งนี้ บริษัทจะไม่รับผิดชอบในกรณีความเสียหายใด ๆ อันเกิดจากการที่เจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่นใดซึ่งได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จงใจหรือประมาทเลินเล่อ หรือเพิกเฉยต่อมาตรการรักษาความปลอดภัย จนเป็นเหตุให้ข้อมูลส่วนบุคคลถูกใช้ หรือเปิดเผยต่อบุคคลที่สามหรือบุคคลอื่นใด

10. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอเข้าถึงข้อมูลส่วนบุคคลของตน ขอรับสำเนา, ขอถอนความยินยอม, คัดค้านการเก็บ การใช้ การเปิดเผย, ขอให้ลบทำลาย, ขอให้ระงับการใช้หรือการลบ, ขอแก้ไขข้อมูลให้เป็นปัจจุบัน, ร้องเรียน หรือขอให้โอนข้อมูลส่วนบุคคลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยอัตโนมัติ เว้นแต่เป็นการกระทบต่อสิทธิเสรีภาพของบุคคลอื่น หรือเป็นการปฏิบัติหน้าที่เพื่อสาธารณะประโยชน์หรือตามกฎหมาย หรือเพื่อการศึกษาวิจัย ทั้งนี้ เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ บริษัทจะจัดให้มีกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และต้องทำการบันทึกการดำเนินการตามคำขอและการปฏิเสธคำขอ

11. การร้องเรียน การแจ้งเบาะแส

กรณีพบเหตุอันควรสงสัยหรือเชื่อว่ามีการละเมิดการเก็บรวบรวม ใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลประสงค์ที่จะร้องเรียนหรือใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามนโยบายฉบับนี้ หรือตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล สามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทตามข้อมูลติดต่อด้านล่างนี้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
บริษัท ซีพี ออลล์ จำกัด (มหาชน)
เลขที่ 313 อาคาร ซี.พี. ทาวเวอร์ ชั้น 24 ถนนสีลม แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500
Email Address: privacy@cpall.co.th
เบอร์โทรศัพท์: 02-826-7744

12. **การฝึกอบรม**

บริษัทจัดให้มีการฝึกอบรมและประเมินผลเกี่ยวกับการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้กับผู้บริหารและพนักงานทุกระดับ ในการนี้ ผู้ประสานงานข้อมูลส่วนบุคคล (Data Protection Coordinator : DPC) ต้องเข้าร่วมฝึกอบรมและกำหนดให้พนักงานในสังกัดของตนซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลต้องเข้าร่วมฝึกอบรมอย่างเคร่งครัด

13. **การทบทวนนโยบาย**

บริษัทจะทำการทบทวนนโยบายนี้อย่างน้อยปีละ 1 ครั้ง หรือกรณีกฎหมายที่เกี่ยวข้องมีการเปลี่ยนแปลงแก้ไข

14. **การฝ่าฝืน**

บริษัทจะไม่ยอมประนีประนอมในเรื่องการคุ้มครองข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้มีหน้าที่รับผิดชอบในการดำเนินงานเรื่องใดเรื่องหนึ่งตามหน้าที่ของตน ที่เกี่ยวข้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล ละเลยหรือละเว้นไม่สั่งการ หรือไม่ดำเนินการ หรือสั่งการ หรือดำเนินการอย่างใดอย่างหนึ่งในหน้าที่ของตน จนทำให้เกิดการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลโดยผิดวัตถุประสงค์ การละเมิดต่อเจ้าของข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืนนโยบายและแนวปฏิบัติเกี่ยวกับเรื่องข้อมูลส่วนบุคคล และ/หรือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล กำหนด พนักงานผู้นั้นต้องรับโทษทางวินัยตามระเบียบของบริษัท และหากการกระทำผิดดังกล่าวของพนักงานและ/หรือบุคคลใดก่อให้เกิดความเสียหายแก่บริษัทและ/หรือบุคคลอื่นใด บริษัทอาจพิจารณาดำเนินคดีตามกฎหมายเพิ่มเติมต่อไป

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 16 ธันวาคม พ.ศ. 2567 เป็นต้นไป

ประกาศ ณ วันที่ 4 ธันวาคม พ.ศ. 2567

(นายก่อศักดิ์ ไชยรัตมีศักดิ์)

ประธานกรรมการบริหาร