

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน)

เอสซีจีเคารพสิทธิความเป็นส่วนตัวของลูกค้า ผู้ถือหุ้น พนักงานของเอสซีจี และบุคคลต่าง ๆ ที่เกี่ยวข้อง
เอสซีจี และเพื่อให้เกิดความมั่นใจว่าบุคคลดังกล่าวได้รับความคุ้มครองข้อมูลส่วนบุคคล รวมถึงเพื่อให้เอสซีจี
ประมวลผลข้อมูลส่วนบุคคลของบุคคลดังกล่าวให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่ประชุม
คณะกรรมการบริษัทปูนซิเมนต์ไทย จำกัด (มหาชน) ครั้งที่ 237 (2/2563) เมื่อวันที่ 29 เมษายน 2563 จึงอนุมัติให้ใช้
นโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี เพื่อให้เอสซีจีมีหลักเกณฑ์ กติกา มาตรการกำกับดูแล และการ
บริหารจัดการข้อมูลส่วนบุคคลอย่างชัดเจนและเหมาะสม

1. ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้บังคับกับเอสซีจี พนักงานของเอสซีจี และบุคคลที่เกี่ยวข้องกับการ
ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของเอสซีจี

2. คำนิยาม

- 2.1 การประมวลผล (Processing) หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม
บันทึก จัดระบบ ทำโครงสร้าง เก็บรักษา ปรับปรุง เปลี่ยนแปลง คุ้มครอง ใช้ เปิดเผย ส่งต่อ เผยแพร่ โอน ผสม
เข้าด้วยกัน ลบ ทำลาย
- 2.2 ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวตน
ของบุคคลนั้นได้ ไม่ว่าจะทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ IP Address รูปภาพ
เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง ข้อมูลทางพันธุกรรม ข้อมูลทางชีวภาพ (Biometric data)
- 2.3 เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลธรรมดาที่ข้อมูลส่วนบุคคลสามารถระบุตัวตน
ของบุคคลนั้นได้ ไม่ว่าจะทางตรงหรือทางอ้อม
- 2.4 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลธรรมดาหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่
ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- 2.5 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลธรรมดาหรือนิติบุคคลซึ่งดำเนินการ
เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
- 2.6 เอสซีจี หมายถึง บริษัทปูนซิเมนต์ไทย จำกัด (มหาชน) และบริษัทย่อยตามงบการเงินรวมของบริษัท
ปูนซิเมนต์ไทย จำกัด (มหาชน)

3. นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Governance)

- 3.1 เอสซีจีจะจัดให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล เพื่อกำหนดวิธีการและมาตรการที่เหมาะสมในการปฏิบัติตามกฎหมาย ดังนี้
- (1) กำหนดให้มีโครงสร้างองค์กร (Organizational Structure) รวมทั้งกำหนดบทบาท ภารกิจ และความรับผิดชอบของหน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้องให้ชัดเจน เพื่อสร้างกลไกการกำกับดูแล การควบคุม ความรับผิดชอบ การปฏิบัติงาน การบังคับใช้ และการติดตามมาตรการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
 - (2) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเอสซีจี (SCG Data Protection Officer: SCG DPO) โดยมีบทบาทและหน้าที่ตามที่กำหนดในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
- 3.2 เอสซีจีจะจัดทำนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
- 3.3 เอสซีจีจะจัดให้มีกระบวนการบริหารการปฏิบัติตามนโยบาย (Policy Management Process) เพื่อควบคุมดูแลให้มีการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจีอย่างต่อเนื่อง
- 3.4 เอสซีจีจะดำเนินการฝึกอบรมพนักงานของเอสซีจีอย่างสม่ำเสมอ เพื่อให้พนักงานของเอสซีจีตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และทำให้มั่นใจได้ว่าพนักงานของเอสซีจีที่เกี่ยวข้องทุกคนผ่านการฝึกอบรม และมีความรู้ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี

4. นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing)

- 4.1 เอสซีจีจะประมวลผลข้อมูลส่วนบุคคลทั้งในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย เป็นธรรม โปร่งใส และคำนึงถึงความถูกต้องของข้อมูลส่วนบุคคล ทั้งนี้ การกำหนดขอบเขตวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล และระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล ให้ทำได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายและแนวทางการดำเนินธุรกิจของเอสซีจี อีกทั้งเอสซีจีจะดำเนินการรักษาความลับ ความถูกต้องสมบูรณ์ และความปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ
- 4.2 เอสซีจีจะจัดให้มีกระบวนการและการควบคุมเพื่อบริหารจัดการข้อมูลส่วนบุคคลในทุกขั้นตอนให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี

- 4.3 เอสซีจีจะจัดทำและรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคล (Records of Processing: RoP) สำหรับบันทึกรายการและกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมาย รวมทั้งจะปรับปรุงบันทึกการประมวลผลข้อมูลส่วนบุคคลเมื่อมีการเปลี่ยนแปลงรายการหรือกิจกรรมที่เกี่ยวข้อง
 - 4.4 เอสซีจีจะจัดให้มีกระบวนการที่ชัดเจนเพื่อให้มั่นใจได้ว่าการแจ้งวัตถุประสงค์การเก็บรวบรวมและรายละเอียดการประมวลผลข้อมูลส่วนบุคคล (Privacy Notices) และการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสอดคล้องกับกฎหมาย รวมทั้งจัดให้มีมาตรการดูแลและตรวจสอบในเรื่องดังกล่าว
 - 4.5 เอสซีจีจะจัดให้มีกลไกการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล รวมทั้งจัดให้มีกลไกการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
 - 4.6 ในกรณีที่เอสซีจีส่ง โอน หรือให้บุคคลอื่นใช้ข้อมูลส่วนบุคคล เอสซีจีจะจัดทำข้อตกลงกับผู้รับหรือใช้ข้อมูลส่วนบุคคลนั้นเพื่อกำหนดสิทธิและหน้าที่ให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
 - 4.7 ในกรณีที่เอสซีจีส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เอสซีจีจะปฏิบัติให้สอดคล้องกับกฎหมาย
 - 4.8 เอสซีจีจะทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดระยะเวลา โดยปฏิบัติให้สอดคล้องกับกฎหมายและแนวทางการดำเนินธุรกิจของเอสซีจี
 - 4.9 เอสซีจีจะประเมินความเสี่ยงและจัดทำมาตรการเพื่อบรรเทาความเสี่ยง และลดผลกระทบที่จะเกิดขึ้นกับการประมวลผลข้อมูลส่วนบุคคล
5. นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)
- เอสซีจีจะจัดให้มีมาตรการ ช่องทาง และวิธีการเพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนได้ตามที่กฎหมายกำหนด รวมทั้งจะดำเนินการบันทึก และประเมินผลการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
6. นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Personal Data Security)
- 6.1 เอสซีจีจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ รวมทั้งดำเนินการป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลและการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต

6.2 เอสซีจีจะจัดให้มีนโยบายการบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Privacy Incident Management Policy) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Program) เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างทัน่วงที

6.3 เอสซีจีจะจัดให้มีกระบวนการแจ้งเจ้าของข้อมูลส่วนบุคคล รวมถึงเจ้าพนักงานของรัฐ ผู้ควบคุมข้อมูลส่วนบุคคล (ในกรณีที่เอสซีจีเป็นผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน) และบุคคลอื่น ให้สอดคล้องกับกฎหมาย

7. นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการกำกับให้เกิดการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Compliance)

7.1 เอสซีจีจะจัดให้มีกระบวนการติดตามในกรณีที่กฎหมายเปลี่ยนแปลงไป และปรับปรุงมาตรการคุ้มครองข้อมูลส่วนบุคคลให้ทันสมัยและสอดคล้องกับกฎหมายอยู่เสมอ

7.2 เอสซีจีจะจัดให้มีการทบทวนและปรับปรุงนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำ เพื่อให้ทันสมัยสอดคล้องกับกฎหมายและสถานการณ์ในแต่ละช่วงเวลา

8. บทบาท หน้าที่ และความรับผิดชอบ

8.1 คณะกรรมการบริษัท มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

- (1) กำกับให้เกิดโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล และการควบคุมภายในที่เกี่ยวข้องของเอสซีจี เพื่อให้เกิดการปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
- (2) กำกับดูแลและสนับสนุนให้เอสซีจีดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ และสอดคล้องกับกฎหมาย

8.2 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Privacy Committee)

ให้คณะกรรมการบริหารความเสี่ยงของเอสซีจี (Risk Management Committee) ทำหน้าที่เป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

- (1) จัดให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคลและการควบคุมภายในที่เกี่ยวข้อง รวมถึงนโยบายการบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Privacy Incident Management Policy) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Program) เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างทัน่วงที

- (2) ประเมินประสิทธิภาพการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี และรายงานผลการประเมินดังกล่าวให้คณะกรรมการบริษัททราบเป็นประจำอย่างน้อย 1 ครั้งต่อปี รวมถึงควบคุมดูแลให้มั่นใจได้ว่าความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้รับการจัดการและมีแนวทางการบริหารความเสี่ยงที่เหมาะสม
 - (3) กำหนดและทบทวนมาตรฐานการปฏิบัติงาน (Standards) และแนวปฏิบัติ (Guidelines) เพื่อให้การดำเนินงานของเอสซีจีสอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
 - (4) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเอสซีจี (SCG DPO)
- 8.3 ผู้บริหาร มีบทบาท หน้าที่ และความรับผิดชอบในการติดตามควบคุมให้หน่วยงานที่ดูแลปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี และส่งเสริมการสร้างวัฒนธรรมที่ตระหนักรู้ให้เกิดขึ้นกับพนักงานของเอสซีจี
- 8.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเอสซีจี (SCG DPO) มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้
- (1) รายงานสถานะการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบอย่างสม่ำเสมอ และจัดทำข้อเสนอแนะเพื่อปรับปรุงการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจีให้ทันสมัยและสอดคล้องกับกฎหมาย
 - (2) ให้คำแนะนำเอสซีจีและพนักงานของเอสซีจีเพื่อให้สามารถปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจีได้
 - (3) ตรวจสอบการดำเนินงานของเอสซีจี เพื่อให้เกิดการปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี
- 8.5 พนักงานของเอสซีจี มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้
- (1) ปฏิบัติให้สอดคล้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
 - (2) รายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการไม่ปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจีให้ผู้บังคับบัญชาทราบ

9. โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจี

การไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเอสซีจีอาจมีความผิดและถูกลงโทษทางวินัย รวมทั้งอาจได้รับโทษตามที่กฎหมายกำหนด

มีผลบังคับใช้ตั้งแต่วันที่ 30 เมษายน 2563

ตามมติที่ประชุมคณะกรรมการบริษัทปูนซิเมนต์ไทย จำกัด (มหาชน) วันที่ 29 เมษายน 2563

พลอากาศเอก



(สถิตย์พงษ์ สุขวิมล)

ประธานกรรมการ