

ประกาศที่ 05/2569

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล บริษัท โปร อินไซด์ จำกัด (มหาชน)

1. ขอบเขตและวัตถุประสงค์

บริษัท โปร อินไซด์ จำกัด (มหาชน) ("บริษัท") เคารพและให้ความสำคัญต่อสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้า ผู้ถือหุ้น ผู้ใช้บริการเว็บไซต์ บุคคลภายนอก และผู้มีส่วนได้เสียทุกกลุ่ม บริษัทจึงกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางในการเก็บรวบรวม ใช้ เปิดเผย หรือดำเนินการใด ๆ กับข้อมูลส่วนบุคคล (รวมเรียกว่า "การประมวลผล") ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง รวมถึงมาตรฐานและแนวปฏิบัติที่เหมาะสม และสอดคล้องกับมาตรฐาน ISO/IEC 27701:2025 ระบบการจัดการข้อมูลความเป็นส่วนตัว (Privacy Information Management System: PIMS) บริษัทกำหนดมาตรการในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลโดยมิชอบ รวมถึงเพื่อสร้างความเชื่อมั่นให้แก่เจ้าของข้อมูลส่วนบุคคลว่า ข้อมูลของตนได้รับการดูแลและคุ้มครองตามมาตรฐานที่ กฎหมายกำหนด นโยบายฉบับนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของบุคคลที่มีความสัมพันธ์กับบริษัท ทั้งในปัจจุบันและอนาคต ได้แก่ บุคลากร ลูกค้า คู่ค้า ผู้ถือหุ้น ผู้ใช้บริการเว็บไซต์ บุคคลภายนอก ผู้สมัครงาน และผู้มีส่วนได้เสียอื่น รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการแทนหรือในนามของบริษัท โดยบริษัทกำหนดให้ผู้ที่เกี่ยวข้องทุกฝ่ายต้องปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด

- นโยบายนี้วางกรอบหลักการและแนวทางในการดำเนินการที่สำคัญสำหรับการคุ้มครองข้อมูลส่วนบุคคลของบริษัท เพื่อให้การดำเนินงานทั้งปวงเป็นไปตามหน้าที่และความรับผิดชอบของบริษัทในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- นโยบายนี้ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งปวงที่เกิดขึ้นตามขอบเขตและวัตถุประสงค์ของบริษัท ซึ่งรวมถึงการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยบุคคลหรือนิติบุคคลภายนอก หรือโดยอุปกรณ์หรือระบบภายนอกตามขอบเขตและวัตถุประสงค์ดังกล่าวด้วย
- นโยบายนี้ไม่ครอบคลุมถึงการประมวลผลข้อมูลส่วนบุคคลของบุคลากรของบริษัทที่ดำเนินการเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้นอันไม่เกี่ยวข้องกับขอบเขตและวัตถุประสงค์ของบริษัท

บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (PII Controller) จะดำเนินการประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล และจะจัดให้มีมาตรการคุ้มครองข้อมูลตั้งแต่การออกแบบ (Privacy by Design) และโดยค่าเริ่มต้น (Privacy by Default)

2. หลักการคุ้มครองข้อมูลส่วนบุคคล

- การประมวลผลข้อมูลส่วนบุคคลของบริษัทต้องดำเนินการตามหลักการดังต่อไปนี้ (สอดคล้องกับ PDPA มาตรา 21-26 และ ISO/IEC 27701 ข้อ 7.2.1)
- ความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness, Fairness and Transparency): เป็นการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย มีความเป็นธรรม และตรวจสอบได้

2/การจำกัดวัตถุประสงค์.....

- การจำกัดวัตถุประสงค์ (Purpose Limitation): เป็นการประมวลผลข้อมูลส่วนบุคคลภายในขอบเขตและวัตถุประสงค์ที่กำหนดและไม่นำไปใช้หรือเปิดเผยนอกขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูลนั้น
- การเก็บข้อมูลเท่าที่จำเป็น (Data Minimization): เป็นการประมวลผลข้อมูลส่วนบุคคลเป็นไปเท่าที่จำเป็นเกี่ยวข้อง และเพียงพอต่อขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูลนั้น
- ความถูกต้องของข้อมูล (Accuracy): เป็นการประมวลผลข้อมูลส่วนบุคคลที่ถูกต้องและดำเนินการให้ข้อมูลเป็นปัจจุบันในกรณีที่เป็น
- การจำกัดระยะเวลาการเก็บ (Storage Limitation): เป็นการจำกัดเก็บข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็นต่อการประมวลผลข้อมูลนั้น บริษัทจะกำหนดระยะเวลาการเก็บรักษาข้อมูลไว้ในนโยบายการเก็บรักษาข้อมูล (Data Retention Policy)
- ความสมบูรณ์และการรักษาความลับ (Integrity and Confidentiality): เป็นการประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล
- ความรับผิดชอบที่ตรวจสอบได้ (Accountability): บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แสดงให้เห็นว่าการประมวลผลข้อมูลเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลที่กฎหมายกำหนด และสามารถพิสูจน์การปฏิบัติตามได้

3. ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

บริษัทจะประมวลผลข้อมูลส่วนบุคคลทั่วไปตามมาตรา 24 และข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมาตรา 26 โดยอาศัยฐานทางกฎหมายอย่างใดอย่างหนึ่ง ดังต่อไปนี้

- ความยินยอม (Consent) — มาตรา 19: เจ้าของข้อมูลได้ให้ความยินยอมอย่างชัดแจ้ง โดยสมัครใจ มีข้อมูลครบถ้วน และสามารถถอนความยินยอมได้ทุกเมื่อ
- การปฏิบัติตามสัญญา (Contractual Necessity) — มาตรา 24(3): จำเป็นต่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา
- หน้าที่ตามกฎหมาย (Legal Obligation) — มาตรา 24(6): จำเป็นเพื่อการปฏิบัติตามกฎหมายที่บริษัทอยู่ภายใต้บังคับ
- ประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) — มาตรา 24(5): เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัทหรือบุคคลภายนอก โดยไม่กระทบสิทธิขั้นพื้นฐานของเจ้าของข้อมูล
- การป้องกันหรือระงับอันตราย (Vital Interest) — มาตรา 24(2): จำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ

สำหรับข้อมูลอ่อนไหว (Sensitive Data) ตามมาตรา 26: บริษัท จะประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวเฉพาะเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานทางกฎหมายหรือข้อยกเว้นที่กฎหมายกำหนดให้สามารถดำเนินการได้โดยไม่ต้องขอความยินยอม

3/4. ประเภทข้อมูลส่วนบุคคล.....

4. ประเภทข้อมูลส่วนบุคคลที่เก็บรวบรวม

บริษัทอาจเก็บรวบรวมข้อมูลส่วนบุคคลประเภทต่าง ๆ ดังนี้

- ข้อมูลอัตลักษณ์ เช่น ชื่อ-นามสกุล รูปภาพบุคคล เป็นต้น
- ข้อมูลที่อยู่และที่ติดต่อ เช่น ที่อยู่ หมายเลขโทรศัพท์ อีเมล สถานที่ทำงาน เป็นต้น
- ข้อมูลประวัติ เช่น สัญชาติ วันเดือนปีเกิด อายุ เพศ เป็นต้น
- ข้อมูล ID เช่น รหัสประจำตัวพนักงาน เลขประจำตัวประชาชน เลขหนังสือเดินทาง ลายมือชื่อ เป็นต้น
- ข้อมูล IT เช่น User ID, IP Address, GPS Location, ข้อมูลการเข้าใช้งานระบบ และข้อมูล Cookies เป็นต้น
- ข้อมูลเกี่ยวกับการเงิน เช่น เลขที่บัญชีธนาคาร เงินเดือน ข้อมูลการชำระเงิน เป็นต้น
- ข้อมูลเกี่ยวกับการทำงาน เช่น ตำแหน่งงาน สายงาน แผนก ประวัติการทำงาน การลา และข้อมูลที่เกี่ยวข้องกับการปฏิบัติงาน เป็นต้น

นอกจากนี้ ในบางกิจกรรมบริษัทอาจมีความจำเป็นต้องประมวลผล ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลชีวมิติ และข้อมูลประวัติอาชญากรรม ทั้งนี้ บริษัทจะประมวลผลข้อมูลดังกล่าวเฉพาะเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานทางกฎหมายหรือข้อยกเว้นที่กฎหมายกำหนดให้สามารถดำเนินการได้

5. หน้าที่และความรับผิดชอบ

- คณะกรรมการบริษัทมีหน้าที่ในทางบริหารที่จะรับผิดชอบในการดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎที่เกี่ยวข้อง โดยดำเนินการผ่านคณะกรรมการตรวจสอบ ที่มีหน้าที่กำกับดูแลและติดตามการปฏิบัติตามนโยบาย และระเบียบต่าง ๆ ที่เกี่ยวข้อง รวมถึงรับผิดชอบในการสนับสนุนทรัพยากรและโครงสร้างองค์กรที่เพียงพอสำหรับการคุ้มครองข้อมูลส่วนบุคคล (ISO/IEC 27701 ข้อ 5.1)
- ส่วนงานและพนักงานทุกคนมีความรับผิดชอบต้องดำเนินการตามนโยบายนี้โดยมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท และคณะทำงานฯ เป็นผู้ติดตามตรวจสอบและดำเนินการให้เป็นไปตามกฎหมาย พนักงานทุกคนจะต้องผ่านการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ (ISO/IEC 27701 ข้อ 5.3.1)
- กิจกรรมการประมวลผลข้อมูลส่วนบุคคลจะต้องถูกบันทึกไว้ในบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกำหนด ตามข้อกำหนด PDPA มาตรา 39 และ ISO/IEC 27701 ข้อ 7.2.8
- ในกรณีที่มีข้อพิจารณาทางกฎหมายที่เกี่ยวข้อง รวมถึงความจำเป็นต้องมีเอกสาร ข้อตกลง หรือแบบฟอร์มใด ส่วนงานจะต้องหาหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจรวมถึงการปรึกษาร่วมกันกับคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

6. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

มีหน้าที่ดังต่อไปนี้ (สอดคล้องกับ PDPA มาตรา 41-43 และ ISO/IEC 27701 ข้อ 5.4.1)

- กำหนดและติดตามตรวจสอบการดำเนินการตามนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคลของบริษัทเพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎที่เกี่ยวข้อง

4/จัดทำแนวปฏิบัติและคู่มือ.....

- จัดทำแนวปฏิบัติและคู่มือการปฏิบัติตามนโยบายนี้ เพื่อใช้อบรมและเป็นแนวปฏิบัติแก่ส่วนงานและพนักงานต่าง ๆ รวมถึงแนวปฏิบัติการจัดเก็บบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเพื่อให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้
- ให้คำแนะนำแก่ส่วนงานต่าง ๆ รวมทั้งพนักงานของบริษัทเกี่ยวกับการปฏิบัติตามนโยบายนี้
- ตรวจสอบการดำเนินงานของส่วนงานต่าง ๆ รวมทั้งพนักงานของบริษัทเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามนโยบายนี้
- ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัท
- รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามนโยบายนี้
- รายงานไปยังคณะกรรมการบริษัทและประธานเจ้าหน้าที่บริหารโดยตรงในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ตามนโยบายนี้
- สนับสนุนและช่วยเหลือการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของส่วนงานต่าง ๆ
- ให้คำปรึกษาหารือเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และเป็นที่ติดต่อประสานงานสำหรับเจ้าของข้อมูลส่วนบุคคลเพื่อรับคำร้องคำขอและดำเนินการเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ติดตามตรวจสอบและแก้ไขข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- จัดเก็บบันทึกการเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและทำหน้าที่แจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
- บันทึกความเห็นต่อประเด็นหรือต่าง ๆ เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัท
- เป็นที่ติดต่อและประสานงานเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัท
- ดำเนินการอื่น ๆ ตามที่ได้รับมอบหมายตามนโยบายนี้
- DPO ต้องได้รับการสนับสนุนจากผู้บริหารระดับสูงอย่างเพียงพอ มีอิสระในการปฏิบัติหน้าที่ ไม่ถูกกดดันหรือลงโทษจากการปฏิบัติหน้าที่ตามกฎหมาย และต้องมีทรัพยากรที่เพียงพอในการปฏิบัติหน้าที่

7. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

- สิทธิในการถอนความยินยอม (Right to Withdraw Consent) — มาตรา 19 วรรคห้า: ถอนความยินยอมที่เคยให้ไว้ได้ทุกเมื่อ
- สิทธิในการรับทราบ (Right to be Informed) — มาตรา 23: รับทราบรายละเอียดการประมวลผลข้อมูลส่วนบุคคลก่อนหรือขณะที่บริษัทเก็บรวบรวมข้อมูล
- สิทธิในการเข้าถึง (Right of Access) — มาตรา 30: ขอรับสำเนาข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมไว้
- สิทธิในการโอนย้ายข้อมูล (Right to Data Portability) — มาตรา 31: ขอรับข้อมูลในรูปแบบที่สามารถนำไปใช้งานต่อได้

5/สิทธิในการคัดค้าน.....

- สิทธิในการคัดค้าน (Right to Object) — มาตรา 32: คัดค้านการประมวลผลข้อมูลของตน
 - สิทธิในการลบข้อมูล (Right to Erasure) — มาตรา 33: ขอให้ลบหรือทำลายข้อมูลส่วนบุคคล
 - สิทธิในการระงับการใช้ข้อมูล (Right to Restriction of Processing) — มาตรา 34: ขอให้ระงับการใช้ข้อมูลชั่วคราว
 - สิทธิในการแก้ไขข้อมูล (Right to Rectification) — มาตรา 35–36: ขอให้แก้ไขข้อมูลที่ไม่ถูกต้องหรือไม่ครบถ้วน
- บริษัทจะดำเนินการตามคำร้องขอเจ้าของข้อมูลภายใน 30 วันนับจากวันที่ได้รับคำร้อง และจะแจ้งผลการดำเนินการหรือเหตุผลของการปฏิเสธให้ทราบ ทั้งนี้หากท่านเห็นว่าบริษัทไม่ได้ปฏิบัติตามกฎหมาย ท่านมีสิทธิร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้

8. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

หากบริษัทมีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ บริษัทจะดำเนินการดังนี้

- ส่งข้อมูลไปยังประเทศที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศรับรองว่ามีมาตรฐานการคุ้มครองข้อมูลเพียงพอ
- จัดให้มีมาตรการคุ้มครองข้อมูลที่เหมาะสมและบังคับใช้ได้ เช่น ข้อสัญญามาตรฐาน (Standard Contractual Clauses) หรือนโยบายองค์กรที่มีผลผูกพัน (Binding Corporate Rules)
- ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลในกรณีที่ไม่มีการอื่น

9. กรณีละเมิดการคุ้มครองข้อมูลส่วนบุคคล

- เหตุการณ์ละเมิดข้อมูลส่วนบุคคลอาจเกิดขึ้นในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยหรือถูกเข้าถึงได้โดยบุคคลที่ไม่ได้รับอนุญาต หรือกรณีที่ข้อมูลส่วนบุคคลถูกใช้ในลักษณะที่เจ้าของข้อมูลส่วนบุคคลไม่อาจคาดหมายได้โดยชอบตามกฎหมาย
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะดำเนินการตรวจสอบเหตุการณ์ทั้งหลายที่เกี่ยวข้องกับการละเมิดการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย เพื่อดำเนินการมาตรการที่เหมาะสมเพื่อบรรเทาผลกระทบและป้องกันเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่จะเกิดขึ้นในอนาคต

ในกรณีที่สมควรตามสภาพและความร้ายแรงของเหตุการณ์ที่เกิดขึ้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะดำเนินการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ตามหลักเกณฑ์ต่อไปนี้ (สอดคล้องกับ PDPA มาตรา 37(4) และ ISO/IEC 27701 ข้อ 6.13.2)

ผลกระทบต่อสิทธิ และเสรีภาพของ เจ้าของข้อมูลส่วนบุคคล	การดำเนินการ
กรณีไม่มีความเสี่ยง	บันทึกเหตุละเมิดข้อมูลส่วนบุคคล
กรณีมีความเสี่ยง	บันทึกเหตุละเมิดข้อมูลส่วนบุคคล แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
กรณีมีความเสี่ยงสูง	บันทึกเหตุละเมิดข้อมูลส่วนบุคคล แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง แจ้งเจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยเร็ว

6/กรณีที่ไม่สามารถแจ้งเหตุ.....

กรณีที่ไม่สามารถแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง บริษัทจะบันทึกเหตุผลของความล่าช้าไว้เป็นหลักฐาน

- กรณีที่ระบบเทคโนโลยีสารสนเทศหรือกระบวนการที่เกี่ยวข้องไม่สามารถทำงานได้ ให้พนักงานหรือส่วนงานที่พบเหตุแจ้งไปยังฝ่ายเทคโนโลยีสารสนเทศ ภายใน 4 ชั่วโมง นับจากเมื่อทราบเหตุนั้น และให้ฝ่ายเทคโนโลยีสารสนเทศประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อดำเนินการตามที่เหมาะสม
- กรณีที่ไม่ใช่เหตุขัดข้องทางเทคโนโลยีสารสนเทศ ให้พนักงาน หรือส่วนงานที่พบเหตุ แจ้งโดยตรง ไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อดำเนินการตามที่เหมาะสม

10. มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ได้แก่

- มาตรการด้านเทคนิค: การเข้ารหัสข้อมูล (Encryption), การควบคุมการเข้าถึง (Access Control), การบันทึกและตรวจสอบ (Audit Log)
- มาตรการด้านองค์กร: นโยบายการรักษาความลับ, การฝึกอบรมพนักงาน, การบริหารจัดการความเสี่ยง
- มาตรการด้านกายภาพ: การควบคุมการเข้าถึงพื้นที่ประมวลผลข้อมูล, การจัดการเอกสารที่มีข้อมูลส่วนบุคคล
- การประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) — PDPA มาตรา 39 วรรคสาม: ในกรณีที่การประมวลผลมีความเสี่ยงสูง บริษัทจะดำเนินการประเมิน DPIA ก่อนเริ่มประมวลผล
- บริหารจัดการผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor): บริษัทจะทำสัญญาประมวลผลข้อมูล (Data Processing Agreement: DPA) กับผู้ประมวลผลทุกรายตามมาตรา 40 และ ISO/IEC 27701 ข้อ 6.12

11. การปฏิบัติตามนโยบาย

- การละเมิดไม่ปฏิบัติตามนโยบายนี้ และมาตรการที่เกี่ยวข้อง ถือเป็นกรณีผิดวินัยร้ายแรง ซึ่งต้องถูกดำเนินการทางวินัยที่เกี่ยวข้องต่อไป
- พนักงานหรือบุคคลอื่นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตและวัตถุประสงค์ของบริษัทอาจต้องมีความรับผิดชอบในการส่วนตัวตามกฎหมายจากการกระทำของตนตามสภาพและความร้ายแรงของเหตุการณ์ที่เกิดขึ้น

12. การทบทวนและปรับปรุงแก้ไข

ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทบทวนและเสนอปรับปรุงแก้ไขนโยบายนี้และมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยคำนึงถึงหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด รวมถึง กฎ ระเบียบ และประกาศอื่น ๆ ที่อาจมีขึ้นมาในอนาคตที่ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

13. การรายงานเบาะแสหรือข้อร้องเรียน

บริษัทส่งเสริมให้บุคลากร ลูกค้า คู่ค้า ผู้ถือหุ้น ผู้ใช้บริการเว็บไซต์ บุคคลภายนอก และผู้มีส่วนได้เสีย ทุกฝ่ายสามารถแจ้งเบาะแส หรือร้องเรียนเกี่ยวกับ การละเมิดข้อมูลส่วนบุคคล โดยบริษัทจะดำเนินการตรวจสอบข้อเท็จจริงด้วยความเป็นธรรม เก็บรักษาข้อมูลของผู้ร้องเรียนเป็นความลับ และคุ้มครองผู้แจ้งเบาะแสที่กระทำโดยสุจริตผู้ที่ประสงค์จะรายงานเบาะแสหรือร้องเรียน สามารถติดต่อได้ผ่านช่องทางดังต่อไปนี้

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
อีเมล: DPO@proinside.co.th
- ส่งหนังสือมายังบริษัท โปร อินไซด์ จำกัด (มหาชน) เลขที่ 55 อาคาร เอ.เอ.แคปปิตอล รัชดา ชั้น 5 ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
- โทรศัพท์: 0 2029 7875

หากมีข้อสงสัย ต้องการสอบถาม ขอคำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล หรือการปฏิบัติตามนโยบายฉบับนี้ สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทได้ตามช่องทางที่ระบุข้างต้น บริษัทจะตอบกลับคำร้องภายใน 30 วันนับจากวันที่ได้รับคำร้อง

จึงประกาศมาเพื่อทราบโดยทั่วกัน และมีผลตามประกาศ ณ วันที่ 1 กันยายน 2569 เป็นต้นไป

ประกาศ ณ วันที่ 9 กันยายน พ.ศ. 2569



(นางสาวเบญญาภา เฉลิมวัฒน์)
ประธานเจ้าหน้าที่บริหาร
บริษัท โปร อินไซด์ จำกัด (มหาชน)