ระเบียบปฏิบัติการตรวจประเมินภายในระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

บริษัทได้กำหนดแนวทางในการตรวจประเมินภายในของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลของบริษัท เพื่อให้มั่นใจว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามระเบียบปฏิบัติที่กำหนด

1. วัตถุประสงค์

1.1 เพื่อให้การดำเนินการตามระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลของบริษัทเป็นไปตามที่บริษัทกำหนด

1.2 เพื่อให้สามารถระบุโอกาสในการปรับปรุงพัฒนาระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้มีความเหมาะสม เพียงพอในการคุ้มครองข้อมูลส่วนบุคคล

2. ผู้รับผิดชอบ

2.1 ให้ผู้แทนฝ่ายบริหารระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล (DPMR) มีหน้าที่ควบคุมการตรวจประเมินภายในของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

2.2 ให้ DPMR เป็นผู้ตรวจประเมินภายในของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด ยกเว้นข้อกำหนด หรือระเบียบปฏิบัติใดๆ ภายใต้ระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดให้ DPMR เป็นผู้รับผิดชอบข้อกำหนด หรือระเบียบปฏิบัตินั้น หรือผู้ที่ได้รับแต่งตั้งเป็น DPMR เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามระเบียบปฏิบัติใดๆ

2.3 ให้ผู้บังคับบัญชาฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ตรวจประเมินภายในของข้อกำหนด หรือระเบียบปฏิบัติภายใต้ระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลที่ DPMR ไม่มีอำนาจในการตรวจประเมินภายใน

2.4 ให้ DPO เป็นผู้ตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด มีอำนาจเป็นผู้ตรวจสอบภายนอกเพื่อทำให้มั่นใจว่าการคุ้มครองข้อมูลส่วนบุคคลเหมาะสมและเพียงพอ

2.5 ให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลให้ความร่วมมือในการตรวจประเมินภายในของระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

3. ขั้นตอนการตรวจประเมินภายในระบบบริหารจัดการคุ้มครองข้อมูล

3.1 วางแผนการตรวจประเมินระบบคุณภาพภายใน

3.1.1 ให้ DPMR จัดทำแผนการตรวจประเมินภายในระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง โดยแผนการตรวจประเมินจะต้องครอบคลุมหัวข้อต่างๆ ที่กำหนดไว้ในระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล

3.1.2 แจ้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล รวมถึงฝ่ายเทคโนโลยีสารสนเทศ ทราบถึงแผนการตรวจประเมิน เพื่อขอการยืนยันในเรื่องของกำหนดเวลาในการตรวจประเมิน

3.1.3 ผู้ตรวจประเมินจัดเตรียม Check List ให้ครอบคลุมเนื้อหาที่จะทำการตรวจประเมิน

3.2 การดำเนินการตรวจประเมิน

3.2.1 ผู้ตรวจประเมินชี้แจงผู้ควบคุมข้อมูลและผู้ประมวลผล รวมถึงฝ่ายเทคโนโลยีสารสนเทศที่รับการตรวจประเมินให้ทราบถึงวัตถุประสงค์และกำหนดการในการตรวจประเมิน

3.2.2 ข้อบกพร่องที่ตรวจพบระหว่างการตรวจประเมินอันเนื่องมาจากระบบ หรือการปฏิบัติงาน ให้เขียน “ใบคำร้องขอดำเนินการแก้ไข (CAR)” และให้ผู้รับการตรวจประเมินแก้ไขให้แล้วเสร็จภายใน 90 วัน

3.3 สรุปผลและรายงานการตรวจประเมิน

3.3.1 ให้ DPMR รวบรวมรายงานการตรวจประเมินรายงานให้ DPO ทราบ เพื่อใช้เป็นข้อมูลในการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล และรายงานให้ผู้บริหารทราบเพื่อใช้เป็นข้อมูลสำหรับการประชุมทบทวนระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล เพื่อปรับปรุงระบบบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพยิ่งขึ้น