DPO (Data Protection Officer) มีหน้าที่อะไร และต้องรู้อะไรบ้าง

ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีการระบุบทบาทและหน้าที่ของผู้ที่มีส่วนเกี่ยวข้องต่อข้อมูลส่วนบุคคลอยู่หลายตำแหน่ง หนึ่งในนั้นคือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หรือที่มักเรียกย่อว่า DPO โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ บุคคลผู้ได้รับมอบหมายเพื่อทำหน้าที่ดูแล ให้คำแนะนำ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลในองค์กร ให้เป็นไปตามกฎหมายที่ได้กำหนดไว้

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ได้ถูกระบุไว้ในมาตรา 42 ของพระราชบัญญัติ ประกอบด้วย 4 ข้อดังต่อไปนี้

1. ให้คำแนะนำ แก่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ที่เกี่ยวข้อง ยกตัวอย่างเช่น สร้างความตระหนักรู้ (Awareness) ในเรื่องการจัดการข้อมูลส่วนบุคคลอย่างถูกวิธีให้กับพนักงานในองค์กร เช่น จัดอบรมให้ความรู้ PDPA กับคณะทำงานและพนักงานในการใช้ข้อมูลส่วนบุคคลให้ถูกต้องปลอดภัย ตาม PDPA

2. ตรวจสอบการดำเนินงาน เกี่ยวกับการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ที่เกี่ยวข้อง เช่น มีการตรวจสอบว่าองค์กรของเรามีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ถูกต้องครบถ้วนหรือไม่ และมีการละเมิดนโยบายการจัดการข้อมูลส่วนบุคคลเช่นการนำข้อมูลไปใช้นอกเหนือจากวัตถุประสงค์ที่ระบุในประกาศนโยบายการขอคำยินยอมหรือเปล่า

3. ประสานงานและให้ความร่วมมือ กับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (หรือหน่วยงานที่เกี่ยวข้อง) ในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น เมื่อเกิดเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลจากองค์กร ผู้ที่ดำรงตำแหน่งจะเป็นผู้ประสานงานในการออกจดหมายแจ้งเตือนข้อมูลรั่วไหล ให้กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง

4. รักษาความลับ ของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

สิ่งที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องรู้ในเบื้องต้น

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพึงมีความรู้เบื้องต้นใน 3 ประการดังต่อไปนี้

1.พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

DPO เป็นผู้มีหน้าที่ให้คำแนะนำแก่เจ้าหน้าที่ที่เกี่ยวข้องตลอดถึงพนักงานในองค์กร จึงจำเป็นต้องทราบและเข้าใจถึงข้อกำหนดและการปฏิบัติตามข้อกำหนดที่สำคัญใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และทำการฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล รวมไปถึงประกาศของกฎหมายฉบับลูกที่จะตามมาด้วย

2.ความรู้เบื้องต้นเกี่ยวกับเทคโนโลยีสารสนเทศ (IT)

เหตุผลของการประกาศใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มาจากในปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีที่ทำให้การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลทำได้ง่ายขึ้นและสะดวกรวดเร็วกว่าแต่ก่อนมาก ดังนั้น DPO จึงมีความจำเป็นที่ต้องเข้าใจเทคโนโลยีสารสนเทศในเบื้องต้นได้ เช่น ระบบการขอคำยินยอม(consent)ในช่องทางอิเล็กทรอนิกส์, ระบบจัดเก็บข้อมูลที่มีความปลอดภัย, การเข้ารหัสเข้าถึงข้อมูล, กิจกรรมต่างๆที่นำข้อมูลมาประมวลผล ซึ่งล้วนแล้วเกี่ยวข้องกับเทคโนโลยีทางด้านไอทีมากพอสมควรส่วน

3.โครงสร้างองค์กร

DPO ต้องทราบโครงสร้างองค์กร ว่าแผนกใดบุคคลใดเป็นผู้รับผิดชอบในการดูแลและนำข้อมูลส่วนบุคคลไปใช้บ้าง ตลอดจนสามารถเข้าถึงผู้บริหารได้โดยตรงเพื่อรายงานให้ทราบเมื่อเกิดปัญหาข้อมูลส่วนบุคคลรั่วไหล หรือเห็นช่องโหว่ของการดูแลรักษาข้อมูลส่วนบุคคลที่สุ่มเสี่ยงหรือผิดไปจากข้อกำหนดของกฎหมายก็สามารถรายงานต่อผู้บริหารที่มีอำนาจโดยตรงได้เพื่อให้ผลักดันนำไปสู่การเพิ่มเติมนโยบายการดูแลคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรที่รัดกุมต่อไป

สรุป

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล(DPO) มีหน้าที่ดูแลให้คำแนะนำและตรวจสอบเพื่อการคุ้มครองข้อมูลส่วนบุคคล จึงจำเป็นที่ต้องรู้ในกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีความรู้เบื้องต้นในระบบเทคโนโลยีสารสนเทศ(IT) และต้องทราบโครงสร้างขององค์กรที่ตนดำรงตำแหน่งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย