6 คำถามยอดฮิตที่พบบ่อย DPO คือใคร? มีหน้าที่และคุณสมบัติอะไร ตามกฎหมาย PDPA

1) Data Protection Officer หรือ DPO คืออะไร?

เจ้าหน้าที่ DPO ตามกฎหมาย PDPA หรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) คือ บุคคลหลักที่มีบทบาทสำคัญในการดูแลรักษาข้อมูลส่วนบุคคล (Personal Data) ทั้งหมดขององค์กรไม่ว่าจะเป็นทั้งข้อมูลส่วนบุคคลทั้งภายใน เช่น (ข้อมูลพนักงาน) หรือ ภายนอก (ข้อมูลลูกค้า) ตั้งแต่การเก็บจัดเก็บรวบรวม, เปิดเผย, และนำข้อมูลไปใช้รวมไปถึงการกำหนดทิศทางการใช้ข้อมูลส่วนบุคคลให้ปลอดภัยและสอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

2) หน้าที่หลักของ DPO ตามกฎหมายมีอะไรบ้าง?

ตามมาตรา 42 ของ PDPA ได้กำหนดหน้าที่ของตำแหน่งนี้ไว้ ดังนี้

ให้คำแนะนำ PDPA แก่คนในองค์กร

ต้องจัดให้มีการสร้างความตระหนักรู้ (Awareness) ในเรื่องการจัดการข้อมูลส่วนบุคคลอย่างถูกวิธีให้กับพนักงานในองค์กรเช่น การจัดอบรม ให้ความรู้ PDPA กับคณะทำงานและพนักงานเพื่อให้สร้างความตระหนักรู้ในการใช้ข้อมูลส่วนบุคคลให้ถูกต้องปลอดภัย ตาม PDPAตรวจสอบการดำเนินงานคอยตรวจสอบการปฏิบัติตามนโยบายการจัดการข้อมูลส่วนบุคคล เช่น การตรวจสอบว่า องค์กร ของเรามีการบันทึกกิจกรรมการ ประมวลผลข้อมูลส่วนบุคคล (ROPA) ถูกต้อง ครบถ้วนหรือไม่ และมีการละเมิดนโยบายการจัดการข้อมูลส่วนบุคคลเช่นการนำข้อมูลไปใช้นอกเหนือจากวัตถุประสงค์ที่ระบุใน Consent หรือเปล่า? DPO จะเป็นผู้คอย ตรวจสอบ ให้ในส่วนนี้

ประสานงานกับผู้กำกับดูแล

แน่นอนว่าเมื่อเกิดเหตุการณ์ ข้อมูลส่วนบุคคลรั่วไหลจากองค์กร ผู้ที่ดำรงตำแหน่งจะเป็นผู้ประสานงานในการออกจดหมายแจ้งเตือนข้อมูลรั่วไหล ให้กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง

รักษาความลับขององค์กร

สำหรับองค์กร การรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลถือเป็นเรื่องสำคัญมาก เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นจำเป็นที่จะต้องมีหน้าที่รักษาความลับอันได้มาจากการปฏิบัติหน้าที่

3) DPO ต้องมีคุณสมบัติ อะไรบ้าง?

มีความรู้ความเข้าใจใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล รวมถึง กฎหมายอื่นที่เกี่ยวข้อง

แน่นอนว่าการที่จะเข้ามาเป็นตัวแทนในการจัดการข้อมูลส่วนบุคคล ผู้ที่ดำรงตำแหน่งจะต้องมีความรู้และเชี่ยวชาญด้านกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และการควบคุมการใช้ข้อมูลส่วนบุคคลให้ได้ตามที่กฎหมายกำหนด

เป็นนักสื่อสารที่ดี

เนื่องจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องประสานงานกับหน่วยงานอื่น ๆ และทีมต่าง ๆภายในองค์กร ที่มีส่วนเกี่ยวข้องกับกฎหมายนี้ ดังนั้น ต้องเป็นคนที่สามารถอธิบายให้คนในองค์กรเข้าใจภาพรวมของการจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย เพราะจำเป็นต้องมีหน้าที่ เช่น การสัมภาษณ์คณะทำงานต่าง ๆ ที่เก็บข้อมูลส่วนบุคคล ว่า เก็บที่ไหน, มีวัตถุประสงค์อะไรบ้าง, ขอความยินยอมหรือยัง เพื่อมาออกแบบบันทึกกิจกรรมข้อมูลส่วนบุคคล (ROPA) เป็นต้น

มีความรู้เรื่องเกี่ยวกับการบริหารจัดการความปลอดภัยของข้อมูล

นอกจากการเก็บข้อมูลแล้ว การปกป้องข้อมูลไม่ให้รั่วไหลนั้นก็สำคัญเช่นกัน ดังนั้นจะต้องมีความรู้ด้านพื้นฐานด้าน CyberSecurity จึงมีความสำคัญ นอกจากนี้ ถ้าองค์กรไหนที่เก็บข้อมูลส่วนบุคคลในรูปแบบ Digital จะต้องมีมาตรฐานในการเก็บรักษาข้อมูลให้มีความปลอดภัยด้วย ซึ่งเชื่อว่าในอนาคต ประกาศเพิ่มเติมในเรื่องการรักษาความปลอดภัยนี้จะออกตามมาแน่นอน

ไม่ทำหน้าที่อื่นใด ที่ขัดแย้งต่อการปฏิบัติหน้าที่

หมายความว่า ไม่ควรเป็นบุคคลที่ได้รับประโยชน์จากการที่ได้ล่วงรู้ ข้อมูลส่วนบุคคล ตัวอย่างเช่น Sales หรือ Marketing ที่สามารถใช้ประโยชน์จากข้อมูลส่วนบุคคลของลูกค้าได้โดยตรง หรืออีกตัวอย่างหนึ่งคือ นักกฎหมาย เพราะเวลาที่เกิดข้อพิพาทขึ้นมา คนที่ดูแลเรื่องกฎหมายจะต้องเข้าข้างองค์กรอยู่แล้ว “อย่าลืมว่าหัวใจของการทำหน้าที่นี้คือการปกป้องสิทธิของ เจ้าของข้อมูล (Data Subject Right)”

สามารถรายงานผู้บริหารได้โดยตรง

บางครั้งการบริหารภาพรวมข้อมูลของบริษัท ผู้ที่ดำรงตำแหน่งอาจจะเห็นช่องโหว่ของข้อมูลและต้องการจะปรับปรุงแก้ไข ควรจะสามารถรายงานตรงต่อผู้บริหารและผลักดันให้ออกมาเป็นนโยบาย (Privacy Policy) เพื่อที่จะได้ควบคุมจัดการใช้งานข้อมูลได้นั้นเอง

4) สามารถใช้ DPO แบบ Outsource ได้ไหม?

ตามมาตรา 41 ของ PDPA ได้กำหนดหน้าที่ของตำแหน่ง DPO โดยเฉพาะ ดังนี้ ตัวกฎหมายได้บอกชัดเจนอยู่แล้วว่า “DPO หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล อาจเป็นพนักงานของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็นผู้รับให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลข้อมูลส่วนบุคคลก็ได้” ซึ่งในฐานะของเจ้าของข้อมูลส่วนบุคคลนั้น ย่อมเห็นว่ามีความเหมาะสม เพราะตำแหน่งนี้เปรียบเสมือนตัวแทนของเจ้าของข้อมูล ที่จะต้องปกป้องเจ้าของข้อมูลมากกว่าที่จะปกป้องบริษัท แต่ถ้าเป็นคน ภายในองค์กร “อาจจะมีความโน้มเอียงไปทางผลประโยชน์ของบริษัทมากกว่าเจ้าของข้อมูลก็เป็นได้”

สนใจบริการ DPO Outsource Service อ่านรายละเอียดเพิ่มเติมได้ ที่นี่

5) ทำควบตำแหน่งอื่นได้ไหม?

คำตอบ คือ สามารถทำได้ครับ ตราบใดที่ตำแหน่งของคนที่จะเข้ามาเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นไม่ส่งผลกระทบต่องานหลัก อย่างเช่น KPI ไม่สวนทางกัน, การปกป้องค์กรกับเจ้าของข้อมูลแล้วขัดแย้งกัน เป็นต้น

6) องค์กรแบบไหนที่จำเป็นจะต้องมี DPO?

หากสรุปตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะเห็นได้ว่ากิจการหรือองค์กรใดที่จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล องค์กรดังกล่าวจะต้องมีกิจกรรมดังนี้ ข้อใดข้อหนึ่งหรือทั้งหมดก็ได้ อันได้แก่

- เป็นหน่วยงานตามที่หน่วยงานรัฐกำหนด
- ดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (อันได้แก่การเก็บรวบรวม ใช้ และเปิดเผย) อย่างสม่ำเสมอ
- มีการประมวลผลข้อมูลส่วนบุคคลประเภทข้อมูลอ่อนไหว ตามมาตรา 26

ในกรณีองค์กรของท่านไม่ได้เข้าเกณฑ์ข้อกำหนดตาม พ.ร.บ. ทางเราก็มีข้อแนะนำว่าอาจมีการแต่งตั้งตัวแทนในองค์กร เพื่อทำหน้าที่ประสานงานเกี่ยวกับข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลมาขอใช้สิทธิ และเพื่อทำหน้าที่ในการติดต่อประสานงานกับหน่วยงานกำกับดูแลได้นั้นเอง

สรุป : DPO คือใคร? มีหน้าที่อะไรในกฎหมาย PDPA

สำหรับตำแหน่งนี้เปรียบเสมือน Key Player ในการที่จะช่วยให้องค์กรสามารถจัดเก็บ รวบรวม เปิดเผย และใช้ข้อมูลส่วนบุคคล ให้สามารถปฏิบัติตามกฎหมาย PDPA และปกป้องสิทธิของเจ้าของข้อมูลได้อย่างเต็มที่นั้นเอง