KPMG

PDPA Compliance

KPMG in Thailand

PDPA Compliance Journey

1. จัดตั้งทีมงานวางแผนและให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
2. สำรวจการประมวลผลข้อมูลส่วนบุคคลทั่วทั้งองค์กรและจัดทำทะเบียนการประมวลผลข้อมูลส่วนบุคคล
3. ประเมินการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลและจัดทำแผนปรับปรุงการปฏิบัติงานเพื่อให้เป็นไปตามข้อกำหนดของ PDPA
4. จัดทำนโยบายและแนวทางการปฏิบัติงานภายในองค์กร และเอกสารด้านกฎหมายต่างๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
5. จัดหาและติดตั้งเทคโนโลยีเพื่อสนับสนุนการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ และเพิ่มมาตรการรักษาความมั่นคงปลอดภัย
6. จัดให้มีการตรวจสอบกระบวนการปฏิบัติงานระบบงาน รวมถึงมีการปรับปรุงพัฒนาอย่างสม่ำเสมอ

การให้คำปรึกษาเกี่ยวกับ PDPA ของเคพีเอ็มจี

การให้คำปรึกษาสำหรับการปฏิบัติงานให้เป็นไปตามกฎหมาย

- ศึกษาและวิเคราะห์สถานภาพการดำเนินงาน พร้อมจัดทำแนวทางการปรับปรุง (PDPA Gap Assessment)
- จัดเตรียมความพร้อมด้านการปฏิบัติงานภายในให้ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA Process Readiness) ดังนี้
  - โครงสร้างและบทบาทหน้าที่ของผู้เกี่ยวข้อง (PDPA Governance Model)
  - ทะเบียนข้อมูลส่วนบุคคล (Data Inventory) และเส้นทางการไหลของข้อมูลส่วนบุคคล (Data Flow)
  - แนวปฏิบัติและเอกสารประกอบการดำเนินการเพื่อบริหารจัดการสิทธิ์ (DSAR Workflow, Procedure, and Template)
  - แนวปฏิบัติและเอกสารประกอบการดำเนินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Incident Management Guideline)
  - การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)
- ประเมินการปฏิบัติตามกฎเกณฑ์และขั้นตอนการปฏิบัติงานที่กำหนด (PDPA Compliance Audit)
- จัดฝึกอบรมที่เกี่ยวข้อง (PDPA Training)

การให้คำปรึกษาด้านกฎหมาย

- วิเคราะห์และให้คำแนะนำฐานทางกฎหมายที่เหมาะสมสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- จัดเตรียม สอบทาน และ/หรือแก้ไขเอกสารกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น
  - ประกาศความเป็นส่วนตัว
  - หนังสือขอความยินยอม
  - สัญญาประมวลผลข้อมูลส่วนบุคคล
  - สัญญาแบ่งปันข้อมูลส่วนบุคคล
  - ข้อสัญญาและข้อกำหนดในการปฏิบัติตาม PDPA
  - แบบฟอร์มอื่น ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เป็นต้น
- ฝึกอบรมให้ความรู้เกี่ยวกับ PDPA
- ตรวจสอบและประเมินการปฏิบัติตาม PDPA (PDPA Legal Health Check)
- ให้คำปรึกษาทางกฎหมายที่เกี่ยวข้อง

การให้คำปรึกษาด้านเทคโนโลยีและความมั่นคงปลอดภัยทางไซเบอร์

- ศึกษาและวิเคราะห์สถานภาพความปลอดภัยไซเบอร์ พร้อมจัดทำแนวทางการปรับปรุง (Cyber Security Gap Assessment)
- ให้คำแนะนำด้านการติดตั้งระบบปฏิบัติการเพื่อสนับสนุนการปฏิบัติงานด้านการจัดการข้อมูลส่วนบุคคล (PDPA Solution เช่น OneTrust เป็นต้น)
- ให้คำแนะนำด้านการติดตั้งระบบปฏิบัติการเพื่อสนับสนุนการปฏิบัติงานด้านความปลอดภัยไซเบอร์ (Cyber Security Solution เช่น DLP เป็นต้น)

ข้อพิจารณาในการดำเนินการด้าน PDPA

PDPA Compliance

การดำเนินการเพื่อให้สอดคล้องกับกฎหมาย PDPA เป็นความท้าทายอย่างมากโดยเฉพาะองค์กรที่ต้องใช้ข้อมูลส่วนบุคคลจำนวนมากในการดำเนินงาน เพราะทุกหน่วยงานภายในองค์กรที่มีส่วนในประมวลผล (เก็บ ใช้ รวบรวม เปิดเผย และทำลาย) ข้อมูลส่วนบุคคลมีส่วนร่วมในการผลักดันให้เกิดความสำเร็จในการดำเนินการให้เป็นไปตามกฎหมายขององค์กร ดังนั้น การศึกษาทำความเข้าใจกิจกรรมประมวลผลข้อมูลส่วนบุคคลทั่วทั้งองค์กร การสร้างความตระหนักรู้ การจัดทำนโยบายและแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ชัดเจน เพื่อเป็นแนวทางให้พนักงานนำไปใช้ในการปฏิบัติงานได้อย่างถูกต้องเป็นไปตามกฎหมาย ตลอดจนการตรวจสอบเพื่อให้มั่นใจว่านโยบายหรือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสอดคล้องกับกฎหมายที่อาจมีการเปลี่ยนแปลงหรือออกใหม่ รวมถึงประกาศที่เกี่ยวข้อง เข้ากับบริบทขององค์กร และมีการนำไปปฏิบัติอย่างเคร่งครัด จึงเป็นเครื่องมือที่สำคัญในการดำเนินการให้เป็นในตามกฎหมาย PDPA และสร้างความเชื่อมั่น (Trust) ให้กับพนักงานในการปฏิบัติงาน รวมถึงเจ้าของข้อมูลส่วนบุคคลและผู้มีส่วนได้เสียอื่นๆ ขององค์กรอีกด้วย

PDPA Legal

PDPA มีความสำคัญอย่างยิ่งต่อทุกองค์กร ซึ่งจำเป็นต้องใช้ข้อมูลส่วนบุคคลในการดำเนินงานขององค์กร และเนื่องด้วยกฎหมายมีความซับซ้อน ดังนั้น องค์กรต้องจัดทำเอกสารทางกฎหมาย นโยบาย และแนวทางการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจน และให้ความสำคัญกับการฝึกอบรมพนักงานให้มีความรู้ความเข้าใจในกฎหมายและการใช้งานเอกสารต่าง ๆ เพื่อให้พนักงานสามารถปฏิบัติตาม PDPA ได้อย่างถูกต้องและมีประสิทธิภาพ

Privacy Solution

ข้อมูลมีความสำคัญเป็นอย่างยิ่งสำหรับการดำเนินของทุกองค์กร และเป็นอีกหนึ่งกลไกสำคัญในการขับเคลื่อนการดำเนินงานขององค์กร ซึ่งบริบทขององค์กรและพลวัตรการเปลี่ยนแปลงในปัจจุบัน ทำให้องค์กรจะต้องบริหารจัดการกับข้อมูลที่มีจำนวนและความซับซ้อนมากขึ้น รวมถึงกฎหมายออกใหม่ต่างๆ ที่เกี่ยวข้อง โดยเฉพาะข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามกฎหมายอย่างเคร่งครัด ดังนั้น การนำเทคโนโลยีที่เหมาะสมมาใช้เพื่อสนับสนุนการปฏิบัติงาน และการบริหารจัดการและคุ้มครองข้อมูลต่างๆ รวมถึงข้อมูลส่วนบุคคลให้มีประสิทธิภาพและสอดคล้องกับขอ้กำหนดของกฎหมายกำหนด จึงเป็นหนึ่งในประเด็นสำคัญที่องค์กรควรพิจารณาโดยเฉพาะอย่างยิ่งกระบวนการที่ต้องบริหารจัดการข้อมูลจำนวนมาก เช่น การบริหารจัดการความยินยอม การบริหารจัดการสิทธิ์ของเจ้าของข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ การนำเทคโนโลยีมาใช้จะทำให้องค์กรปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ มีข้อมูลสำหรับการติดตามและตรวจสอบได้ง่าย

Cyber Security Solution

การที่องค์กรจะคุ้มครองข้อมูลส่วนบุคคลให้ปลอดภัยในยุคดิจิทัลได้นั้น ปัจจัยหลักที่ขาดไม่ได้คือการมี Cyber Security ที่เข้มแข็ง เพื่อเฝ้าระวัง ป้องกัน และตอบสนองต่อความเสียหายที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูล โดยทุกองค์กรควรพิจารณาวางกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสม โดยครอบคลุมตั้งแต่ระดับนโยบาย ตลอดจนโครงสร้างการปฏิบัติงานที่เกี่ยวข้อง รวมถึงการสร้างความตระหนักรู้แก่บุคลากร และการนำเทคโนโลยีมาประยุกต์ใช้เพื่อให้เกิดสมดุลระหว่างการนำข้อมูลส่วนบุคคลมาใช้ปฏิบัติงานอย่างมีประสิทธิภาพ และการรักษาความมั่นคงปลอดภัยต่อข้อมูลขององค์กร

ติดต่อเรา

ผู้เชี่ยวชาญด้านกระบวนการปฏิบัติงานภายในองค์กร

คุณนัยน์ปพร สกุลญาติ
หุ้นส่วน
T: +66 2677 2313
E: naipaporn@kpmg.co.th

คุณปุณฑริก เพชรคูหา
ผู้ช่วยกรรมการบริหาร
T: +66 2677 2717
E: pundarik@kpmg.co.th

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านไซเบอร์

คุณวาริท นำชัยศิริ
ผู้ช่วยกรรมการบริหาร
T: +66 2677 2796
E: waritn@kpmg.co.th

ผู้เชี่ยวชาญด้านกฎหมาย PDPA

คุณวิภาพรรณ จตุพรหมวงศ์
กรรมการบริหาร
T: +66 2677 2515
E: vipaphan@kpmg.co.th

คุณภัทรพร กายบริบูรณ์
ผู้ช่วยกรรมการบริหาร
T: +66 2677 2514
E: pattarapornk@kpmg.co.th

kpmg.com/th

Twitter: @KPMG_TH
LinkedIn: kpmg-Thailand
Facebook: KPMGinThailand
YouTube: kpmginthailand
Instagram: kpmgthailand