DDTI KNOWLEDGE SHARING PERSONAL DATA PROTECTION

คู่มือเตรียมความพร้อมสำหรับ PDPA (ฉบับสถานศึกษา)

คำแนะนำสำหรับสถานศึกษา เพื่อการดำเนินการตามกฎหมาย และการจัดการข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

โดย บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัด และ สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

สารบัญ

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) ประกาศลงในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 ส่งผลให้เกิดความตื่นตัวในแทบทุกวงการ ไม่เว้นแม้แต่ “วงการการศึกษา” โดยกฎหมายฉบับนี้มีผลกระทบต่อการเก็บรวบรวม ใช้ และเปิดเผย (การประมวลผล) ข้อมูลส่วนบุคคลในสถานศึกษา ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลหลากหลายบทบาทหน้าที่ ไม่ว่าจะเป็นบุคลากร นักเรียน พ่อแม่ผู้ปกครอง ตลอดจนผู้เกี่ยวข้องกลุ่มอื่น

สถานศึกษาเป็น “ผู้ควบคุมข้อมูล” (Data Controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (PDPA มาตรา 6) จึงมีภาระหน้าที่ตามบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคล จำเป็นต้องศึกษา วางแผน และดำเนินการให้มีมาตรฐานและมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

คู่มือเตรียมความพร้อมสำหรับ PDPA (ฉบับสถานศึกษา) เล่มนี้ จัดทำขึ้นเพื่อแนะนำแนวทางการดำเนินงานเพื่อคุ้มครองข้อมูลส่วนบุคคลขององค์กรสถานศึกษาที่มีความซับซ้อน โดยมีประเด็นหลักๆ ที่ควรให้ความสำคัญมากถึง 10 ประการ ด้วยหวังเป็นอย่างยิ่งว่า เอกสารฉบับนี้จะเป็นประโยชน์แก่ผู้อ่านในวงการการศึกษาและผู้ที่สนใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในบริบทของสถานศึกษา

**เนื้อหาบางส่วนอ้างอิงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) เนื่องจากเป็นกฎหมายแม่แบบของ PDPA ที่มีบังคับใช้มาเป็นระยะเวลาหนึ่ง และมีข้อบังคับเพิ่มเติมจากหน่วยงานคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุม*

หากมีข้อผิดพลาดหรือไม่สมบูรณ์ประการใด ทางสถาบันฯ ต้องขออภัยมา ณ ที่นี้
สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

รายละเอียดช่องทางการติดต่อ
บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัด – Digital Business Consult Co.,Ltd. (DBC)
www.digitalbusinessconsult.asia
สถาบันทดสอบและพัฒนาทักษะดิจิทัล – Digital Skill Development and Testing Institute (DDTI)
www.ddti.org
หลักสูตร ICDL Personal Data Protection Certificate (ICDL PDPC)
https://pdpa.online.th/
Facebook Fanpage: PDPA ICDLThailand
LINE: @pdpathailand

กรณีที่ 1: การติดต่อสื่อสารกับผู้ปกครอง นักเรียน หรือบุคลากร

การจัดสรรความรับผิดชอบ

บุคลากร/เจ้าหน้าที่ระดับสูงของสถานศึกษาควรเป็นผู้รับผิดชอบในการบริหารจัดการเกี่ยวกับการติดต่อสื่อสารใด ๆ ที่ถูกส่งออกไปในนามขององค์กร (ไม่ว่าจะเป็นการใช้กระดาษหรือเอกสารสั่งทำเฉพาะที่มีตราสัญลักษณ์ หรือสามารถระบุตัวตนขององค์กรในฐานะผู้ส่งด้วยวิธีการอื่น) ซึ่งนี่ไม่ได้หมายความว่าคุณควรจัดให้มีบุคคลเพียงคนเดียวที่เป็นผู้ส่งสารทางการทั้งหมดขององค์กร อย่างไรก็ตาม ผู้ที่ส่งสารในนามขององค์กรทุกคนควรทราบว่า ในการติดต่อสื่อสารกับผู้ปกครอง นักรียน หรือบุคลากร ซึ่งมีการใช้ข้อมูลส่วนบุคคลจะต้องดำเนินอย่างสอดคล้องตาม PDPA

ข้อความบริการ vs ข้อความการตลาด

สถานศึกษาสามารถบ่งบอกความแตกต่างระหว่าง “ข้อความบริการ” และ “ข้อความการตลาด” ได้ โดย

- “ข้อความบริการ” คือ การสื่อสารที่จำเป็นเกี่ยวกับการจัดการภารกิจในแต่ละวันของสถานศึกษา ซึ่งผู้ปกครองและนักเรียนคาดหวังว่าจะได้รับเป็นปกติอยู่แล้ว (เช่น การแจ้งเตือนเกี่ยวกับการสอบ กำหนดการเปิด-ปิดรับลงทะเบียน การเปลี่ยนแปลงวันหรือเวลานัดหมายประชุมผู้ปกครอง วันเปิดทำการของสถานศึกษาที่กำลังจะมาถึง เป็นต้น)
- “ข้อความการตลาด” คือ การสื่อสารเชิงส่งเสริมการตลาด ซึ่งสถานศึกษาส่งถึงผู้ปกครอง/นักเรียนเพื่อโปรโมตหรือโฆษณาผลิตภัณฑ์ บริการ หรือบัตรสำหรับเข้าชมงานของสถานศึกษาเป็นต้น

หากมีการแจ้งให้นักเรียนและผู้ปกครองทราบตั้งแต่ช่วงของการลงทะเบียนเข้าสถานศึกษาแล้ว การสื่อสารข้อความบริการสามารถกระทำได้โดยไม่จำเป็นต้องได้รับความยินยอมล่วงหน้า อย่างไรก็ตาม ด้านข้อความการตลาด GDPR บัญญัติไว้ว่า สถานศึกษาจะต้องได้รับความยินยอมล่วงหน้าที่มีลักษณะชัดแจ้ง และให้โดยไม่ต้องมีสิ่งตอบแทนจากบุคลากรและ/หรือผู้ปกครองก่อนการส่งสารอิเล็กทรอนิกส์เพื่อวัตถุประสงค์ทางการตลาด ตามที่อธิบายไว้ข้างต้น ส่วน PDPA ก็มีบัญญัติว่า การขอความยินยอมจะต้องกระทำโดยชัดแจ้ง เป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ ด้วยเช่นเดียวกัน

ข้อควรปฏิบัติ

- สำหรับการสื่อสารทางไปรษณีย์ สถานศึกษา/องค์กรควรมีหัวจดหมายทางการ และอนุญาตเฉพาะบุคลากร/เจ้าหน้าที่ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงทรัพยากรนี้ เพื่อควบคุมจำนวนของผู้ที่เป็นตัวแทนขององค์กรหรือสื่อสารในฐานะตัวแทนขององค์กร
- ผู้ที่ส่งสารในนามขององค์กรควรดำเนินการให้แน่ใจว่า ครูใหญ่/ผู้อำนวยการ/ผู้บริหารองค์กรรับรู้และให้การอนุมัติเห็นด้วยก่อนการสื่อสารออกไปในทุก ๆ ครั้ง
- ผู้ที่ได้รับมอบหมายให้เป็นผู้ส่งสารการตลาดทางตรงหรือโปรโมชั่นรูปแบบอิเล็กทรอนิกส์ ไม่ว่าจะเป็นผ่านทางอีเมล SMS หรือโซเชียลมีเดีย ควรดำเนินการให้แน่ใจว่าได้รับความยินยอมจากผู้ที่คาดว่าเป็นผู้รับสารล่วงหน้า โดยความยินยอมจะต้องให้โดย “ระบุวัตถุประสงค์ชัดเจน ไร้ข้อกำกวม และเจ้าของข้อมูลสามารถเลือกได้อย่างอิสระ”
- ข้อความสื่อสารการตลาดทางตรงหรือโปรโมชั่น จะต้องมีตัวเลือกหรือฟังก์ชันให้ “ถอนความยินยอม” เพื่อปฏิเสธการรับสารลักษณะดังกล่าวอีกในอนาคต
- การสื่อสารผ่านการรับ-ส่งด้วยมือ (เช่น การฝากเอกสารกับนักเรียนไปให้ผู้ปกครอง) หรือการส่งสารที่ไม่ได้ระบุถึงบุคคลใดโดยเฉพาะ (เช่น ครอบครัว) ไม่จำเป็นต้องดำเนินการอย่างสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- การสื่อสารใด ๆ ในนามขององค์กรควรระบุรายละเอียดติดต่อของผู้ส่งหรือสมาชิกในทีมคนอื่นๆ ด้วย ในกรณีที่ผู้รับสารต้องการความชัดเจนหรือติดตามผล
- สถานศึกษาควรเน้นย้ำความถูกต้องและการขอความยินยอมใช้ข้อมูลรายละเอียดติดต่อของสมาชิกโรงเรียน ณ จุดลงทะเบียน – รวมถึงข้อมูลของผู้ปกครองที่อาจได้รับการติดต่อไปในกรณีของเด็กนักเรียนที่ยังไม่บรรลุนิติภาวะ
- การส่งข้อความบริการผ่านทางกรุ๊ปบนโซเชียลมีเดียหรือแอปพลิเคชันแชท ต้องคำนึงและควบคุมให้เนื้อหาสารที่ส่งออกไปมีความสอดคล้องกับวัตถุประสงค์ของการก่อตั้งกลุ่มนั้น ซึ่งตรงกับบัญญัติของ PDPA ที่ว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือในขณะที่เก็บรวบรวม (PDPA มาตรา 21)
- อีเมลทางการขององค์กรที่ถูกส่งหาผู้รับหลายคนในครั้งเดียว จะต้องใช้ฟังก์ชัน Bcc (Blind Carbon Copy) เสมอ! เพื่อป้องกันไม่ให้ข้อมูลที่อยู่อีเมลของผู้รับถูกเปิดเผยต่อคนอื่นๆ โดยไม่จำเป็น
- สถานศึกษาควรตระหนักว่าในบางกรณีครอบครัวหรือผู้ปกครองของนักเรียนอาจไม่ได้อยู่ด้วยกันอีกต่อไปแล้ว (หย่าร้างหรือแยกกันอยู่) องค์กรควรมีมาตรการให้แน่ใจว่าครอบครัวหรือผู้ปกครองทั้ง 2 ท่าน ได้รับการติดต่อ/ข้อมูลข่าวสารที่เกี่ยวข้องกับลูก (ยกเว้นมีการตกลงกัน) ตามหลักการของ PDPA ที่ระบุว่า ผู้ควบคุมข้อมูลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (PDPA มาตรา 35)
- ข้อความบริการที่เกี่ยวข้องกับกิจกรรมของนักเรียนที่ยังไม่บรรลุนิติภาวะ (อายุต่ำว่า 20 ปีบริบูรณ์) ควรถูกส่งไปยังผู้ปกครองของเด็กเหล่านั้น ไม่ใช่ตัวนักเรียนโดยตรง

ข้อควรหลีกเลี่ยง

- สถานศึกษาควรงดเว้นการส่งโปรโมชั่น การระดมเงินทุน และข้อความทางการตลาดไปยังบุคคลที่มีอายุต่ำกว่า 20 ปีบริบูรณ์
- การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (PDPA มาตรา 19) สถานศึกษาจึงไม่ควรใช้งาน “กล่องตัวเลือกที่คลิกเลือกตั้งต้นให้อัตโนมัติ” ในแบบฟอร์มการสมัครหรือลงทะเบียน

กรณีที่ 2: การลงทะเบียนเข้าร่วมกิจกรรม

การจัดสรรความรับผิดชอบ

ครูใหญ่/ผู้อำนวยการ/ผู้บริหารองค์กร และเลขานุการ ควรเป็นผู้รับผิดชอบหลักในการบริหารจัดการและดำเนินกระบวนการลงทะเบียนใด ๆ ภายในสถานศึกษา หัวหน้าชั้นปีและบุคลากรคนอื่นๆ อาจเป็นผู้เก็บรวบรวมข้อมูลโดยตรงจากนักเรียนและผู้ปกครอง อย่างไรก็ตาม กระบวนการโดยรวมยังคงเป็นความรับผิดชอบของสถาบันการศึกษาในฐานะนิติบุคคลและผู้ควบคุมข้อมูล

ด้านการจัดการแบบฟอร์มสำหรับสมัครหรือลงทะเบียน ควรออกแบบให้ได้รับข้อมูลครบถ้วนจากนักเรียนและผู้ปกครอง (ในกรณีที่นักเรียนยังไม่บรรลุนิติภาวะ) เพื่อให้ตรงตามวัตถุประสงค์ขององค์กร ขณะเดียวกันก็ควรเก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นเพื่อให้ตอบวัตถุประสงค์ดังกล่าว

ข้อควรปฏิบัติ

- ออกแบบแบบฟอร์มการสมัคร/ลงทะเบียนให้มีช่องสำหรับกรอกข้อมูล (เท่าที่จำเป็น) เพื่อตอบสนองต่อวัตถุประสงค์การเก็บข้อมูลอย่างครบถ้วน
- ระบุรายละเอียดติดต่อของเจ้าหน้าที่คุ้มครองข้อมูล (DPO) หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในช่วงของแบบฟอร์มที่เห็นว่ามีความเหมาะสม เพื่อให้ผู้ที่สมัครหรือลงทะเบียนสามารถติดต่อองค์กรได้ในกรณีที่ต้องการความกระจ่างชัด
- แนะนำให้องค์กรแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นผู้รับผิดชอบดูแลการเก็บรวบรวม การจัดการข้อมูลของผู้สมัคร และให้คำแนะนำเกี่ยวกับที่อาจเป็นประโยชน์ต่อการประมวลผลข้อมูลดังกล่าว แม้สถานศึกษาไม่ได้เป็นองค์กรที่ถูกกำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลตามที่ระบุไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคลล (PDPA มาตรา 41) ก็ตาม
- หากสถานศึกษาของคุณเป็นเครือธุรกิจหรือเครือกิจการเดียวกัน อาจแต่งตั้ง “เจ้าหน้าที่คุ้มครองข้อมูลร่วม” เป็นบุคคลเดียวได้ โดยทุกสถานทำการจะต้องสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย
- ณ จุดลงทะเบียน (หรือหน้าเข้าลงทะเบียนในกรณีออนไลน์) นักเรียนและผู้ปกครองจะต้องได้รับการบอกกล่าวว่า ข้อมูลส่วนบุคคลของพวกเขาจะถูกนำไปใช้งานภายใต้วัตถุประสงค์ใด
- หากมีพื้นที่เพียงพอ คุณควรเขียนบรรยายสั้น ๆ ในแต่ละส่วนของแบบฟอร์มลงทะเบียนเพื่ออธิบายถึงเหตุผลว่าทำไมข้อมูลนั้น ๆ จึงต้องถูกเก็บรวบรวม พร้อมระบุถึงกระบวนการใช้งานและเปิดเผยข้อมูล เพื่อสร้างความเข้าใจและความคาดหวังที่เป็นเหตุเป็นผลของผู้กรอกแบบฟอร์ม
- กรณีนักเรียนที่ยังไม่บรรลุนิติภาวะ แบบฟอร์มลงทะเบียนควรมีส่วนที่แยกออกมาอย่างชัดเจนสำหรับผู้ปกครองโดยเฉพาะ สำหรับการ “เลือกรับ” ข้อมูลเกี่ยวกับโปรโมชั่นและกิจกรรมระดมทุนต่าง ๆ โดยจะต้องให้ผู้ให้ความยินยอมทำเครื่องหมายหรือคลิกยอมรับเองอย่างอิสระ (ไม่สามารถใช้กล่องที่ทำเครื่องหมายให้ล่วงหน้าได้) ซึ่งหากผู้ปกครองไม่ให้ความยินยอม องค์กรควรมีมาตรการให้แน่ใจว่าบุคคลเหล่านี้จะไม่ได้รับการติดต่อถึงด้วยเหตุผลดังกล่าว
- ทันทีที่กรอกและส่งมอบเรียบร้อย สถานศึกษาควรเรียบเรียงและลำเลียงแบบฟอร์มทั้งหมดไปยังสถานที่เก็บรักษากลางขององค์กรอย่างรวดเร็วที่สุด และหากเป็นไปได้ก็ควรพยายามลดการเก็บข้อมูลในรูปแบบเอกสารกระดาษลงให้ได้มากที่สุดด้วยเช่นกัน โดยอาจแปลงและย้ายข้อมูลจากเอกสารแบบฟอร์มกระดาษที่นักเรียนและผู้ปกครองกรอกเข้ามาเข้าสู่ระบบคอมพิวเตอร์ เนื่องจากมีความปลอดภัย และประสิทธิภาพที่สูงกว่าในแง่ของการจัดเก็บ การจัดการ การประมวลผล และการเรียกข้อมูลเพื่อใช้งาน
- หากมีการพิมพ์ข้อมูลจากเอกสารกระดาษเข้าสู่ระบบคอมพิวเตอร์ขององค์กร เมื่อเรียบร้อยแล้ว แบบฟอร์มกระดาษในตอนแรกควรถูกเก็บรักษาอย่างปลอดภัยหรือไม่ก็ถูกฉีกทำลายตามหลักการ สถานศึกษาควรปรับปรุงนโยบายการจัดการกับข้อมูลที่เกิดขึ้นในลักษณะนี้เพื่อกระตุ้นให้เกิดแนวทางปฏิบัติงานที่ดีในระยะยาว

ข้อควรหลีกเลี่ยง

- คุณจะต้องไม่ขอข้อมูลแบบหว่าน นอกเหนือจากที่ต้องการจากนักเรียนหรือผู้ปกครอง (หรือผู้ปกครองที่ใช้อำนาจแทนนักเรียน) ผ่านแบบฟอร์มสมัคร/ลงทะเบียน หากยังไม่มีความจำเป็นในการประมวลผลข้อมูลนั้น
- การจัดทำแบบฟอร์ม ไม่ควรเขียนกำกับช่องว่างสำหรับกรอกข้อมูลใด ๆ ว่า “จำเป็น” นอกเหนือจากเป็นข้อบังคับอย่างเป็นทางการหรือข้อบังคับตามบทกฎหมาย ซึ่งหากมีการระบุฯ ก็ควรอธิบายถึงข้อกำหนดของกฎหมายที่เกี่ยวข้องกับข้อมูลดังกล่าวนั้นประกอบด้วย

- องค์กรสถานศึกษาจะต้องไม่อนุมานเอาเองว่าผู้ปกครองหรือบุคลากรจะอยากได้รับข่าวสารทางด้านการตลาดหรือโปรโมชั่น เพียงเพราะพวกเขาเกี่ยวข้องกับองค์กรหรือมีลูกเรียนอยู่ที่นี่ แบบฟอร์มขอประมวลผลข้อมูลเพื่อวัตถุประสงค์ทางการตลาดจากบุคคลเหล่านี้จะต้องให้พวกเขาเป็นผู้ “เลือกรับ” ข่าวสารอย่างอิสระด้วยตนเองเช่นเดียวกับบุคคลอื่น ๆ (ไม่ใช่ตัวเลือกที่จะปฏิเสธที่จะไม่รับข่าวสาร)

กรณีที่ 3: การขอให้เปิดเผยข้อมูลส่วนบุคคล

การจัดสรรความรับผิดชอบ

หลายครั้งหลายคราว สถานศึกษาอาจจำเป็นต้องให้หรือเปิดเผยข้อมูลของบุคลากรหรือนักเรียน เมื่อตกอยู่ในสถานการณ์ดังกล่าว องค์กรจะต้องแสดงความรับผิดชอบในฐานะผู้ควบคุมข้อมูลและจัดวางมาตรการสำหรับการขอเข้าถึงข้อมูลส่วนบุคคลที่เข้มแข็ง โดยจะสามารถเปิดเผยข้อมูลตามคำขอได้หากสถานศึกษาได้พิสูจน์แล้วว่าคำขอนั้นสามารถกระทำได้ มีความเหมาะสมและสอดคล้องตามฐานทางกฎหมาย

ข้อควรปฏิบัติ

- ผู้อำนวยการ ผู้บริหารระดับสูง หรือบุคลากรของสถานศึกษาที่ได้รับมอบหมายให้รับผิดชอบตอบสนองต่อคำขอประเภทนี้ ควรเป็นผู้ที่พิจารณาว่าคำขอเพื่อเข้าถึงข้อมูลส่วนบุคคลที่เก็บรักษาโดยองค์กรนั้น ๆ ตกอยู่ภายใต้ฐานทางกฎหมายใด
- และแม้ว่าคำขอเข้าถึงข้อมูลดังกล่าวจะสามารถกระทำได้และสอดคล้องตามกฎหมาย สถานศึกษาควรเปิดเผยข้อมูลอย่างน้อยที่สุดเท่าที่จำเป็น เพียงพอเฉพาะเพื่อดำเนินการตามคำขอเข้าถึงข้อมูลที่มีเข้ามาเท่านั้น
- บุคลากรของสถานศึกษาควรทราบเกี่ยวกับข้อกฎหมาย หรือพันธะผูกพันตามกฎหมายที่อาจนำมาใช้อนุญาตให้องค์กรเปิดเผยข้อมูลส่วนบุคคลของนักเรียนได้ในการดำเนินกิจการตามปกติ
- สถานศึกษาควรทำหน้าที่เป็น “ผู้รักษาประตู” กำกับดูแลการใช้งานหรือการเปิดเผยข้อมูลที่เก็บรักษาโดยองค์กร

ข้อควรหลีกเลี่ยง

- ข้อมูลส่วนบุคคลของบุคลากรหรือนักเรียนไม่ควรสามารถเข้าถึงได้โดยทั่วไป
- ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้คำปรึกษาหรือการสนับสนุนของสถาบันไม่ควรถูกเปิดเผยนอกเสียจากได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล (หรือผู้ปกครองในกรณีเป็นผู้เยาว์) หรือได้รับอนุญาตตามอำนาจทางกฎหมาย
- องค์กรสถานศึกษาไม่ควรเปิดเผยข้อมูลส่วนบุคคลนอกเสียจากได้รับแบบฟอร์มคำขออย่างเป็นลายลักษณ์อักษร
- องค์กรสถานศึกษาไม่ควรเปิดเผยข้อมูลส่วนบุคคลของบุคลากร นักเรียน หรือผู้ปกครองไม่ว่าจะเป็นรายบุคคลหรือหลาย ๆ คนพร้อมกัน ให้กับองค์กรอื่น นอกเสียจากมีเหตุชอบด้วยกฎหมาย

กรณีที่ 4: การจัดการความยินยอม

การจัดสรรความรับผิดชอบ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง PDPA การประมวลผล (เก็บรวบรวม ใช้ และเปิดเผย) ข้อมูลส่วนบุคคลกระทำได้โดยชอบ หากองค์กรสามารถอ้างอิงฐานทางกฎหมายสำหรับการประมวลผลข้อมูลนั้น ๆ โดย “ความยินยอม” เป็น 1 ใน 7 ฐานการประมวลผลข้อมูล

องค์กรจำเป็นต้องได้รับความยินยอมเพื่อประมวลผลข้อมูลโดยชอบตามกฎหมาย หากไม่สามารถอ้างฐานการประมวลผลอื่นมารองรับได้ โดยในบริบทของสถานศึกษา อาจจำเป็นต้องขอความยินยอมจากนักเรียนซึ่งมีสถานะเป็นผู้เยาว์ โดยการขอความยินยอมจากผู้เยาว์ที่ยังไม่บรรลุนิติภาวะให้ดำเนินการ ดังนี้ (PDPA มาตรา 20)

- ผู้เยาว์อายุ 11-19 ปี ให้ขอความยินยอมจากตัวผู้เยาว์เอง และจากพ่อแม่ผู้ปกครองร่วมด้วย
- ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจากพ่อแม่ผู้ปกครองของผู้เยาว์

ภายใต้ PDPA การขอความยินยอมต้องกระทำโดยชัดแจ้ง เป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ โดยต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย และต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีรูปแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ นอกจากนั้นต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (PDPA มาตรา 19) หากการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลของสถานศึกษาไม่เป็นไปตามที่กำหนดไว้ข้างต้น ก็จะไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และสถานศึกษาไม่อาจดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ขอความยินยอมได้

ข้อควรปฏิบัติ

- สถานศึกษาควรบอกกกล่าวแนะนำพ่อแม่ผู้ปกครองและตัวนักเรียนเอง เกี่ยวกับกิจกรรมหรือบริการ (เช่น การให้คำปรึกษาของโรงเรียน) ที่มีการขอความยินยอมเกิดขึ้นเมื่อเปิดรับสมัครหรือลงทะเบียน
- แบบฟอร์มหรือเอกสารใด ๆ ที่กรอกโดยนักเรียนและ/หรือพ่อแม่ผู้ปกครอง ควรถูกเก็บรักษาในแฟ้มข้อมูลที่เกี่ยวข้องกับนักเรียนเป็นรายบุคคล พร้อมจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อเป็นการรักษาความลับของเจ้าของข้อมูลและผู้เกี่ยวข้อง
- ความยินยอมที่ถูกให้เอาไว้ก่อนหน้า พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะบังคับใช้ หรือก่อน 27 พฤษภาคม 2562 อาจไม่สอดคล้องกับข้อบังคับของกฎหมาย สถานศึกษาควรติดต่อกลับไปยังผู้ให้ความยินยอม ไม่ว่าจะเป็นบุคลากร นักเรียน หรือผู้ปกครอง เพื่อยืนยันการให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของพวกเขาอีกครั้งหนึ่ง (ขอความยินยอมใหม่) ด้วยแบบฟอร์มขอความยินยอมฉบับปรับปรุงให้สอดคล้องตาม PDPA เรียบร้อยแล้ว
- ความยินยอมควรได้รับการทบทวนและขอ “ต่อ” ความยินยอมออกไปอีกอย่างน้อยปีละ 1 ครั้ง เพื่อยืนยันว่าเจ้าของข้อมูลยังคงเต็มใจที่จะเข้าร่วมในกิจกรรมหรือยังคงต้องการรับบริการต่อไป

ข้อควรหลีกเลี่ยง

- สถานศึกษาไม่ควรอนุมานว่าความยินยอมจะคงอยู่ตลอดไป โดยต้องวางมาตรการ/กระบวนการทบทวน ปรับปรุง และให้เจ้าของข้อมูลส่วนบุคคลต่อความยินยอมอย่างน้อยปีละ 1 ครั้ง
- ความยินยอมต่อกิจกรรมหรือบริการหนึ่ง ไม่อาจนำมาคาดเดาเหมารวมว่าเจ้าของข้อมูลส่วนบุคคลจะให้ความยินยอมต่อบริการอื่น ๆ ที่มีความคล้ายคลึงกันได้ หากองค์กรสถานศึกษาต้องการนำเสนอกิจกรรมหรือบริการอื่น ๆ จะต้องจัดทำแบบฟอร์มขอความยินยอมแยกออกจากกันเป็นเรื่อง ๆ อย่างชัดเจน

กรณีที่ 5: การเก็บรักษาบันทึกข้อมูลและการลบทำลาย

การจัดสรรความรับผิดชอบ

สถานศึกษาจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลบางประเภทเอาไว้เป็นระยะเวลาที่แตกต่างกันออกไป ด้วยเหตุผลเช่น เพื่อให้บริการด้านการลงทะเบียนและธุรการ เพื่อความสอดคล้องตามพันธะของกฎเกณฑ์หรือกฎหมาย หรือเพื่อเก็บรักษาบันทึกประวัติของทางองค์กร เป็นต้น โดยสถานศึกษาจะต้องพยายามหาสมดุลระหว่างการเก็บรักษาข้อมูลเพื่อประโยชน์ขององค์กร และการลดความเสี่ยงด้านข้อมูล ด้วยการลบหรือทำลายข้อมูลที่ไม่มีความจำเป็นสำหรับการดำเนินงานขององค์กรอีกต่อไป

ด้วยเทคโนโลยีการจัดเก็บแบบอิเล็กทรอนิกส์อย่างในสมัยนี้ องค์กรสามารถจัดเก็บข้อมูลได้อย่างยาวนานด้วยงบประมาณที่ต่ำมาก ส่วนบันทึกเอกสารกระดาษอาจใช้พื้นที่มากและอาจเป็นภาระที่น่ารำคาญหากไม่ได้รับการจัดระเบียบอย่างเหมาะสม มีประสิทธิภาพ และเก็บรักษาอย่างมั่นคงปลอดภัย

หลักสำคัญหนึ่งของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง PDPA ก็คือ องค์กรควรเก็บรักษาข้อมูลเอาไว้เป็นระยะเวลาเพียงเท่าที่จำเป็นภายใต้รูปแบบที่สามารถระบุตัวตนของบุคคลได้ เพื่อบรรลุวัตถุประสงค์ด้านการดำเนินงานและตามภาระผูกพันตามกฎหมาย (เช่น งานทะเบียนธุรการสมาชิก ข้อผูกพันการประเมินผลการจ้างงานและเงินเดือน การรายงานไปยังรัฐบาลและหน่วยงานระดับชาติอื่น ๆ การเก็บรักษาข้อมูลเพื่อวัตถุประสงค์ทางประกันหรือกฎหมาย ฯลฯ) โดยเมื่อหมดความจำเป็นในการเก็บรักษา ข้อมูลส่วนบุคคลจะต้องถูกลบ ทำลาย หรือทำให้เป็นนิรนามโดยสมบูรณ์ (PDPA มาตรา 33)

โดยหลักการดังกล่าวไม่เกี่ยวกับเครือข่ายทางไอที ขีดความสามารถของระบบ หรือพื้นที่จัดเก็บข้อมูลที่เหลืออยู่ขององค์กรสถานศึกษา แต่ประเด็นคือบันทึกข้อมูลส่วนบุคคลจะสามารถถูกลบหรือทำลายได้อย่างรวดเร็วที่สุดเมื่อใด

ข้อควรปฏิบัติ

- องค์กรสถานศึกษา (และแต่ละแผนกที่เกี่ยวข้องกับข้อมูล) ควรทราบเกี่ยวกับข้อบังคับทางกฎหมายเกี่ยวกับระยะเวลาการเก็บรักษาบันทึกข้อมูลทางธุรการ สวัสดิการสังคม และการเงิน
- สถานศึกษาควรร่างนโยบายการเก็บรักษาและทำลายข้อมูล และจัดทำตารางระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละประเภทที่กำลังถูกประมวลผลโดยองค์กร ตามข้อกำหนดทางกฎหมายหรือแนวทางการเก็บรักษาข้อมูลของแต่ละหมวดหมู่
- ผู้บริหาร/ผู้จัดการ ผู้อำนวยการ หรือบุคลากรของสถานศึกษา ที่มีสิทธิ/ได้รับอนุญาตให้สามารถเข้าถึงบันทึกข้อมูลส่วนบุคคลได้ ควรทราบเกี่ยวกับนโยบายการเก็บรักษาและทำลายข้อมูล และกลุ่มคนเหล่านี้ควรดำเนินการให้แน่ใจว่าบันทึกข้อมูลนั้น ๆ ถูกเก็บรักษาเอาไว้ไม่เกินระยะเวลาที่ควรจะเป็น โดยที่อ้างอิงกับนโยบายและตารางกำหนดเวลาการเก็บรักษา
- สถานศึกษาต้องคำนึงเสมอว่าข้อกำหนดเกี่ยวกับระยะเวลาการเก็บรักษาข้อมูลบังคับใช้กับทั้งบันทึกข้อมูลในระบบอิเล็กทรอนิกส์และแบบเอกสารกระดาษ

- บันทึกข้อมูลส่วนบุคคลของบุคลากร นักเรียน และผู้ปกครอง บางครั้งอาจถูกนำไปประมวลผลนอกสถานที่ แต่ก็ควรถูกเก็บรวบรวมกลับมาไว้ภายในศูนย์เก็บข้อมูลของสถานศึกษาโดยไม่รอช้า เพื่อการเก็บรักษาในระยะยาวและการลบหรือทำลายหากหมดวัตถุประสงค์ในการประมวลผล
- เมื่อบรรลุวัตถุประสงค์การประมวลผลขององค์กรสถานศึกษาแล้ว เอกสารใด ๆ ที่มีข้อมูลส่วนบุคคล ไม่ว่าจะเป็นจดหมายหรือใบกำกับภาษีเก่า แบบฟอร์มการสมัครลงทะเบียน ฯลฯ ควรถูกนำไปทำลายให้เป็นชิ้นเล็กชิ้นน้อย ก่อนจะถูกนำไปทิ้งในสถานที่ที่เหมาะสม
- บันทึกข้อมูลฉบับจริงสมควรถูกเก็บรักษาเอาไว้ ณ สถานที่เก็บส่วนกลางของสถานศึกษาที่มีความมั่นคงปลอดภัย มากกว่าจะกระจายอยู่ตามแผนกต่าง ๆ หรืออยู่ที่หลายบุคคล
- อุปกรณ์คอมพิวเตอร์ที่ถูกใช้สำหรับการประมวลผลข้อมูลโดยสถานศึกษา ควรถูกล้างสนามแม่เหล็กด้วยแม่เหล็กแรงสูงเพื่อลบร่องรอยต่าง ๆ ของข้อมูล ก่อนอุปกรณ์จะถูกขาย ยกเลิกการใช้งาน หรือถูกนำไปรีไซเคิล
- หากต้องพึ่งพาบริการจัดการข้อมูลจากองค์กร Third-Party ในการจัดเก็บ กู้คืน หรือทำลายข้อมูล สถานศึกษาจะต้องมีสัญญาข้อตกลงการประมวลผลข้อมูล ก่อนหน้าการใช้บริการจากองค์กรภายนอกเหล่านั้น

ข้อควรหลีกเลี่ยง

- องค์กรจะต้องไม่เก็บรักษาบันทึกข้อมูลส่วนบุคคลเอาไว้ยาวนานเกินกว่ากำหนดการที่ตกลงกัน
- บอร์ดบริหาร ผู้อำนวยการ และ/หรือบุคลากร ไม่ควรเก็บรักษาสำเนาบันทึกข้อมูลส่วนบุคคลขององค์กรเอาไว้ที่บ้านพักอาศัยของตนเอง เมื่อบันทึกข้อมูลชุดนั้นฉบับจริงถูกลบทำลายไปแล้วตามนโยบายการเก็บรักษาและลบทำลายข้อมูล
- เราควรตระหนักไว้เสมอว่าสถานศึกษา/องค์กรที่มีสถานะเป็นผู้ประมวลผลข้อมูล จะต้องเป็นผู้รับผิดชอบสูงสุดเกี่ยวกับการเก็บรวบรวม เก็บรักษา ความมั่นคงปลอดภัย และระยะเวลาการเก็บรักษาของข้อมูลส่วนบุคคล โดยไม่ควรมีบุคลากรคนใดคนหนึ่ง (ไม่ว่าประจำหรือสัญญาจ้าง) ที่ลบทำลายหรือจัดทำข้อมูลส่วนบุคคลให้เป็นนิรนามโดยไม่ได้แจ้งและได้รับความเห็นชอบจากผู้บริหารขององค์กร
- เอกสารกระดาษที่มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวต่าง ๆ ไม่ควรแค่ถูกโยนทิ้งลงในถังขยะ แต่สมควรถูกทำลายให้เป็นชิ้นเล็กชิ้นน้อยอย่างปลอดภัยก่อนถูกทิ้งทุกครั้ง
- อุปกรณ์คอมพิวเตอร์ซึ่งใช้ประมวลผลข้อมูลส่วนบุคคลไม่ควรถูกขายทิ้งหรือส่งไปรีไซเคิลโดยไม่ได้รับการ “ล้าง” ข้อมูลส่วนบุคคลออกจากฮาร์ดไดร์ฟโดยมืออาชีพ

กรณีที่ 6: การใช้ภาพถ่ายและวิดีโอ

ภาพถ่ายและวิดีโอสามารถบันทึกลักษณะต่าง ๆ ทางกายภาพของบุคคล จึงนับเป็นข้อมูลส่วนบุคคลที่องค์กรต้องดำเนินการคุ้มครอง/บริหารจัดการให้สอดคล้องตามตาม PDPA (รวมถึง GDPR หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องฉบับอื่น ๆ)

การจัดสรรความรับผิดชอบ

สถานศึกษาที่บันทึกภาพหรือวิดีโอและเก็บรักษาตัว Footage เอาไว้ มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล และจะต้องดำเนินการเพื่อให้แน่ใจว่าการประมวลผลภาพต่าง ๆ ขององค์กรเป็นไปอย่างเหมาะสมและสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อควรปฏิบัติ

- หากสถานศึกษาวางแผนจะเก็บภาพของกิจกรรมหรือการแข่งขันต่าง ๆ ที่กำลังจะจัดขึ้น ผู้เข้าร่วมงานควรได้รับการแจ้งเตือนล่วงหน้าเมื่อสามารถกระทำได้ เช่นอาจแทรกลงในโปสเตอร์หรือบัตรสำหรับเข้างานว่า “ภาพ/วิดีโอที่ถูกถ่ายในงานอาจถูกนำไปใช้โปรโมตและประชาสัมพันธ์ในอนาคต” เป็นต้น
- ณ สถานที่จัดกิจกรรม แนะนำให้สถานศึกษามีการติดโปสเตอร์เป็นระยะ ๆ ให้สามารถสังเกตเห็นได้ เพื่อย้ำเตือนผู้เข้าร่วมว่าจะมีการถ่ายภาพ/วิดีโอ
- อาณาเขตของสถานศึกษาที่มีกล้องวงจรปิด CCTV ควรติดป้าย/ประกาศเตือนว่ามีการบันทึกภาพเอาไว้ให้สามารถมองเห็นได้อย่างชัดเจน เพื่อเป็นการแจ้งให้บุคลากร ผู้ปกครอง และนักเรียนทราบ โดยระบุวัตถุประสงค์ พร้อมรายละเอียดติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้บริหารระดับสูงขององค์กรที่รับผิดชอบ ในกรณีที่มีข้อสงสัยหรือความกังวลใจ
- ระบบวงจรปิด CCTV ควรได้รับการตรวจสอบดูแลอยู่เป็นประจำ เพื่อเช็กดูว่าภาพที่บันทึกได้ถูกนำไปใช้ตรงกับวัตถุประสงค์ของการติดตั้ง และเพื่อป้องกันหรือตรวจสอบกิจกรรมที่ไม่สอดคล้องกับกฎหมาย ตลอดจนการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ช่างภาพที่เก็บภาพถ่าย/วิดีโอจากงานกิจกรรมของสถานศึกษาควรทราบว่า องค์กรต้องการนำภาพหรือวิดีโอของบุคคลใดบ้างไปใช้งาน และควรแจ้งผู้ถูกถ่ายถึงวัตถุประสงค์ของการถ่ายและขอความยินยอมในการใช้งานข้อมูลด้วยเสมอ โดยในกรณีเด็กหรือผู้เยาว์ต้องขอความยินยอมจากผู้ปกครองซึ่งองค์กรอาจเป็นผู้ดำเนินการขอความยินยอมเองในภายหลัง (ก่อนการใช้ข้อมูล)
- แม้ความยินยอมไม่จำเป็นต้องอยู่ในรูปแบบของเอกสารที่เป็นลายลักษณ์อักษรเสมอไป แต่การขอความยินยอมจากผู้ถูกถ่ายภาพ/วิดีโอของช่างภาพก็ควรมีลักษณะที่ชัดเจน เข้าใจง่าย และไม่กำกวม เพื่อหลีกเลี่ยงหรือป้องกันความขัดแย้งในอนาคตเกี่ยวกับการทำข้อมูลภาพถ่าย/วิดีโอไปใช้งานในอนาคต
- ก่อนกิจกรรมหรือการแข่งขันใด ๆ องค์กรสถานศึกษาจะต้องทำสัญญาข้อตกลงการประมวลผลข้อมูลกับช่างภาพมืออาชีพที่จ้าง และระบุมาตรการ/มาตรฐานเกี่ยวกับการเก็บรวบรวม ใช้ และการเก็บรักษาข้อมูลภาพถ่าย/วิดีโอที่จะเกิดขึ้นภายในงาน
- ภาพถ่ายและวิดีโอควรถูกเก็บโดยแบ่งแยกด้วยกิจกรรม/การแข่งขัน และจำแนกตามบุคคลอีกชั้นหนึ่ง เผื่อในอนาคตมีการดึงภาพมาเปิดเผยหรือใช้งาน (ตามวัตถุประสงค์ที่เคยได้ขอความยินยอม)

ข้อควรหลีกเลี่ยง

- ภาพถ่ายและวิดีโอที่ถูกถ่ายในงานกิจกรรมของสถานศึกษาไม่ควรนำไปเผยแพร่โดยปราศจากการรับรู้จากบุคคลในภาพ แม้เป็นการยากที่จะได้รับอนุญาต (ความยินยอม) จากทุกคนในภาพคนกลุ่มใหญ่ ๆ แต่องค์กรก็ควรพยายามทำให้พวกเขารับรู้ล่วงหน้าว่าภาพถ่ายหรือวิดีโอจะถูกโพสต์ลงบนเว็บไซต์หรือโซเชียลมีเดียของสถานศึกษา หรือแจ้งเตือนว่าภาพของพวกเขาอาจถูกนำไปใช้งานเพื่อวัตถุประสงค์ดังกล่าว
- บุคลากรไม่ควรสามารถเปิดหรือเข้าถึงภาพถ่ายและวิดีโอ (รวมถึงภาพจาก CCTV) อย่างไม่มีข้อจำกัด เพื่อเป็นการป้องกันและลดความเสี่ยงของการใช้ภาพอย่างไม่ได้รับอนุญาตหรือเกินวัตถุประสงค์

กรณีที่ 7: ความเกี่ยวข้องกับผู้ให้บริการ Third-Party

สถานศึกษาอาจจำเป็นต้องใช้บริการจากผู้เชี่ยวชาญเฉพาะทางภายนอกองค์กรซึ่งเป็นผู้ให้บริการบุคคลที่สาม (Third-Party) เพื่อช่วยเหลือในการทำงานในหลากหลายโอกาส ยกตัวอย่างเช่น บริษัท Headhunter สรรหาบุคลากรและผู้เชี่ยวชาญ บริษัทจัดการบัญชีดูแลเงินเดือนบุคลากร สำนักงานที่ปรึกษาทางจิตวิทยาสำหรับช่วยเหลือนักเรียน หรือผู้ให้บริการด้านไอทีที่ดูแลเครือข่ายและโครงสร้างพื้นฐาน เป็นต้น

องค์กร/บริษัทผู้ให้บริการบุคคลที่สามข้างต้นจะมีสิทธิและความสามารถเข้าถึงข้อมูลส่วนบุคคลของสถานศึกษาได้ จึงถือว่าเป็น “ผู้ประมวลผลข้อมูล” สถานศึกษาจะต้องดำเนินการจัดทำ “สัญญาข้อตกลงการประมวลผลข้อมูล” ไม่ว่าในรูปแบบเอกสารกระดาษหรืออิเล็กทรอนิกส์กับบริษัทเหล่านี้อย่างเป็นทางการก่อนเริ่มต้นรับบริการ (PDPA มาตรา 40)

การจัดสรรความรับผิดชอบ

ผู้ให้บริการ Third-Party อาจจัดทำ Template ของสัญญาข้อตกลงการประมวลข้อมูลของตนเองเตรียมเอาไว้ อย่างไรก็ตาม หน้าที่ความรับผิดชอบในการจัดการให้สัญญามีผลผูกมัดอย่างสมบูรณ์นั้นขึ้นอยู่กับผู้ควบคุมข้อมูล (ซึ่ง ณ ที่นี้คือสถานศึกษา/ทีมผู้บริหารของสถานศึกษา) เป็นสำคัญ

ข้อควรปฏิบัติ

- สถานศึกษาควรเช็กให้แน่ใจว่าผู้ให้บริการ Third-Party มีมาตรฐานการให้บริการที่มีความชำนาญ ไว้วางใจได้ และสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น ๆ ที่เกี่ยวข้องกับองค์กร
- สถานศึกษาจะต้องแน่ใจว่ามีสัญญาข้อตกลงการประมวลผลข้อมูลที่มีผลบังคับสมบูรณ์ก่อนหน้าที่ผู้ให้บริการ Third-Party จะสามารถเข้าถึงข้อมูลส่วนบุคคลใด ๆ ที่สถานศึกษารับผิดชอบดูแลอยู่
- สัญญาข้อตกลงการประมวลผลข้อมูลควรได้รับการทบทวนเป็นประจำ อย่างน้อยปีละ 1 ครั้ง และผู้ควบคุมข้อมูลจะต้องดูแลให้แน่ใจว่าผู้ประมวลผลข้อมูลดำเนินงานตามข้อตกลงภายใต้สัญญาอย่างครบถ้วนทุกข้อ
- หากผู้ประมวลผลข้อมูลมีการจ้างงานองค์กรอื่นเพื่อให้ความช่วยเหลือในการประมวลผลข้อมูล (ผู้รับจ้างรายย่อย) จะต้องแจ้งสถานศึกษา/องค์กรผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษรเกี่ยวกับการจ้างงานนั้น โดยสถานศึกษา/องค์กรผู้ควบคุมข้อมูลจะต้องมีทางเลือกที่จะปฏิเสธหรือแสดงข้อคิดเห็นอันขัดแย้งต่อการจ้างงานได้

ข้อควรหลีกเลี่ยง

- ผู้ให้บริการ Third-Party ไม่ควรได้รับอนุญาตให้สามารถเข้าถึงเครือข่าย ไฟล์เอกสาร หรืออาคารสำนักงานที่เก็บข้อมูลของสถานศึกษา (ผู้ควบคุมข้อมูล) โดยปราศจากการกำกับดูแลอย่างใกล้ชิด แม้เพียงเป็นระยะเวลาสั้น ๆ หากยังไม่ได้ทำสัญญาข้อตกลงการประมวลผลข้อมูลระหว่างกัน
- เมื่อเสร็จสิ้นความสัมพันธ์ระหว่างกันตามสัญญา ผู้ให้บริการ Third-Party ไม่ควรได้รับอนุญาตให้เก็บข้อมูลที่ถูกเปิดเผยโดยองค์กรสถานศึกษาเอาไว้ โดยควรโอนย้ายข้อมูลคืนหรือลบทำลายข้อมูล เว้นเสียแต่มีพันธะผูกพันทางกฎหมายหรือความจำเป็นต้องเก็บรักษาต่อภายใต้วัตถุประสงค์การดำเนินงานบางประการ
- สถานศึกษาไม่ควรติดต่อผู้ให้บริการ Third-Party เป็นผู้ประมวลผลข้อมูลให้กับองค์กรเพียงเพราะได้รับคำแนะนำมา แต่ต้องมีขั้นตอนของการตรวจเช็กและประเมินขีดความสามารถ คุณสมบัติ และมาตรฐานการดำเนินงานว่าสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง PDPA หรือไม่ ก่อนการทำสัญญาและจ้างงาน

กรณีที่ 8: การจัดการด้านความมั่นคงปลอดภัยข้อมูล

ความล้มเหลวในการปกป้องคุ้มครองข้อมูลส่วนบุคคลให้ปลอดภัยเป็นหนึ่งในสาเหตุหลักที่ส่งผลให้เกิดการละเมิด ซึ่งสร้างความเสียหายต่อองค์กรอย่างมหาศาล เนื่องจากทำลายความเชื่อมั่นของผู้คนที่มีต่อองค์กร กระทบต่อชื่อเสียงและความน่าเชื่อถือของพนักงานและกระบวนการจัดการข้อมูลขององค์กร

การจัดสรรความรับผิดชอบ

บุคลากรระดับสูงของสถานศึกษาควรเป็นผู้รับผิดชอบหลักเกี่ยวกับข้อมูลที่ถูกเก็บรักษาโดยองค์กร ควบคุมว่ามีบุคคลใดที่สามารถเข้าถึงได้ เก็บรักษาไว้ที่ใด และถ่ายโอนหรือโอนย้ายไปที่อื่นด้วยวิธีการใดอย่างไร โดยบุคลากร/เจ้าหน้าที่ที่สามารถเข้าถึงข้อมูลได้ทุกคนจะต้องนึกคำนึงถึงความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และบริหารจัดการข้อมูลซึ่งเป็นสินทรัพย์อันมีค่ายิ่งด้วยความเคารพ ไม่ว่าจะเป็นข้อมูลที่อยู่ในรูปแบบเอกสารกระดาษหรืออิเล็กทรอนิกส์ก็ตาม

การจัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลของแต่ละองค์กรนั้นแตกต่างกันขึ้นอยู่กับจำนวน มูลค่า และรูปแบบของข้อมูลที่เก็บรักษา โดยสถานศึกษาอาจมีมาตรการอย่างเช่น การเข้ารหัสข้อมูล (Encryption) ข้อมูลบนคอมพิวเตอร์แล็ปท็อป สมาร์ทโฟน และอุปกรณ์เก็บข้อมูลต่าง ๆ การตั้งพาสเวิร์ดเพื่อปกป้องไฟล์ทั้งหมดที่เก็บรักษาข้อมูลอ่อนไหว และการใส่กุญแจตู้เก็บเอกสารในสำนักงานเมื่อไม่ได้มีการใช้งาน เป็นต้น

องค์กรควรพิจารณาแบ่งประเภทของข้อมูลออกจากกันอย่างชัดเจน เพื่อจะได้ปรับใช้มาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมกับชุดข้อมูลที่เกี่ยวข้องกับด้านการแพทย์หรือด้านสภาวะทางจิตใจของนักเรียนหรือบุคลากร กล่าวคือ ข้อมูลจำพวกบันทึกการสัมภาษณ์และการให้คำปรึกษาควรได้รับการคุ้มครองในระดับสูงสุด ควบคู่กับการคุ้มครองข้อมูลส่วนบุคคลทางกายภาพในพื้นที่ของสถานศึกษาไม่ว่าจะเป็นการจำกัดจำนวนผู้ถือกุญแจเข้าถึงพื้นที่เก็บข้อมูล ตลอดจนการติดกล้อง CCTV เพื่อดูแลสอดส่องสถานที่ดังกล่าว

ข้อควรปฏิบัติ

- สถานศึกษาควรมีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลที่แสดงให้เห็นถึงระเบียบขององค์กรในการนำข้อมูลไปใช้ การจัดเก็บ การโอนย้าย และใครบ้างที่มีสิทธิหรืออำนาจเข้าถึงข้อมูล
- บุคลากรผู้ที่มีสิทธิเข้าถึงข้อมูลทุกคนควรได้รับการฝึกอบรมเกี่ยวกับภาระหน้าที่ของตน ให้คุ้นเคยกับนโยบายด้านความปลอดภัย และสามารถประมวลผลข้อมูลภายใต้มาตรฐานที่เหมาะสม
- หลังสิ้นสุดระยะเวลาของการเปิดเผยหรือใช้งานข้อมูลส่วนบุคคล (ที่ได้รับความยินยอมล่วงหน้า) บุคลากร/เจ้าหน้าที่ควรถูกเทรนให้เก็บเอกสารหรือสิ่งที่มีข้อมูลส่วนบุคคลเหล่านั้นกลับสู่สำนักงานบริหารของสถานศึกษา หรือพื้นที่เก็บรักษาข้อมูลขององค์กรอย่างรวดเร็วที่สุด
- หลาย ๆ ครั้ง บุคลากรของสถานศึกษาก็จำเป็นต้องถือครองข้อมูลส่วนบุคคลเอาไว้ที่ตนเองเพื่อบริหารจัดการนักเรียนภายในห้องเรียนและเพื่อเตรียมการสอน (ลิสต์รายชื่อนักเรียน รายละเอียดการติดต่อผู้ปกครอง) โดยไม่อาจหลีกเลี่ยงได้ อย่างไรก็ตาม บันทึกข้อมูลควรถูกเก็บรักษาไว้เท่าที่จำเป็น และควรถูกรักษาไว้อย่างปลอดภัยขณะถูกโอนย้ายหรือกำลังถูกใช้งานโดยเฉพาะเวลาเข้าร่วมการประชุมนอกสถานที่ เป็นต้น
- สถานศึกษาควรสำรองข้อมูล (Backup) เอาไว้ในรูปแบบอิเล็กทรอนิกส์ เพื่อที่จะได้สามารถดำเนินการตามปกติได้อย่างทันท่วงทีหากเกิดเหตุภัยพิบัติ (อย่างความเสียหายจากไฟไหม้หรือน้ำท่วม) ขึ้นกับสำนักงาน
- ผู้บริหารระดับสูงควรรับทราบถึงระดับการเข้าถึงข้อมูลนักเรียนและผู้ปกครองของบุคลากร โดยบุคลากรที่สามารถเข้าถึงข้อมูลได้ควรมีหน้าที่เฉพาะเจาะจงที่เกี่ยวข้องกับชุดข้อมูลนั้น
- หากองค์กรมีการจ้างวานบริษัท Third-Party ในการจัดการข้อมูล ควรมีการทำสัญญาข้อตกลงการประมวลผลข้อมูลอย่างเป็นทางการก่อนข้อมูลส่วนบุคคลใด ๆ ขององค์กรจะถูกเปิดเผยต่อบริษัทนั้น
- คอมพิวเตอร์ขององค์กรควรได้รับการปกป้องด้วยพาสเวิร์ด พาสเวิร์ดไม่ควรถูกแชร์ระหว่างบุคลากรของสถานศึกษา หรือทิ้งเอาไว้ให้สามารถเข้าถึงได้โดยง่าย
- องค์กรสถานศึกษาควรปรับใช้นโยบายเคลียร์ “โต๊ะสะอาด” ในพื้นที่ เก็บล็อกแฟ้มเอกสารทุกหลังการทำงานในแต่ละวันหรือเมื่อไม่ได้ใช้งาน และล็อกประตูเข้า-ออกไม่มีผู้อำนาจหน้าที่เกี่ยวข้องกับข้อมูลอยู่ประจำสำนักงาน
- บุคลากรควรล็อกหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อลุกออกจากโต๊ะทำงาน แม้จะเป็นเพียงระยะเวลาสั้น ๆ
- เมื่อมีผู้ออกจากงานหรือย้ายองค์กร ความสามารถในการเข้าถึงข้อมูลของบุคคลนั้นควรถูกถอดถอนหรือเปลี่ยนแปลงอย่างเหมาะสมอย่างรวดเร็วที่สุดเท่าที่จะเป็นไปได้
- การฝึกอบรมควรถูกจัดขึ้นเป็นประจำอย่างเหมาะสม เพื่อกระตุ้นบุคลากรในทุกระดับของสถานศึกษาเกี่ยวกับด้านการคุ้มครองข้อมูล
- หากคุณมีการติดตั้งกล้อง CCTV ในพื้นที่ของสถานศึกษา ผู้บริหารระดับสูง (ที่เกี่ยวข้อง) ควรได้รับความไว้วางใจให้เป็นผู้ดูแลด้านการจัดการและการซ่อมบำรุงของระบบและอุปกรณ์อย่างใกล้ชิด

ข้อควรหลีกเลี่ยง

- ผู้ที่สามารถเข้าถึงข้อมูลไม่ควรเก็บข้อมูลไว้ในอุปกรณ์ที่ปราศจากการเข้ารหัสและระบบรักษาความปลอดภัย เช่น คอมพิวเตอร์หรือสมาร์ทโฟนส่วนตัวที่ไม่ได้ใส่พาสเวิร์ดเข้าเครื่อง
- และหากเป็นไปได้ หลีกเลี่ยงการใช้เครือข่ายสาธารณะเพื่อจัดการหรือสื่อสารข้อมูลส่วนบุคคล โดยควรใช้เครือข่ายเฉพาะ/ส่วนตัวที่มีระบบการเข้ารหัสและมีการรักษาความปลอดภัยสูง
- เอกสารกระดาษไม่ควรถูกโยกย้ายออกจากสำนักงานขององค์กร/สถานศึกษานอกเสียจากมีความจำเป็นที่ไม่สามารถหลีกเลี่ยงได้เท่านั้น สำเนาเอกสารข้อมูลเมื่อใช้งานเสร็จควรถูกเก็บรวบรวมกลับสู่สำนักงานอย่างรวดเร็วที่สุด และหากมีสำเนาเหลือใช้หรือไม่ได้ใช้งานแล้วควรถูกทำลายทิ้งทันทีหลังจากเสร็จสิ้นกิจกรรมหรือวัตถุประสงค์

กรณีที่ 9: การจัดการเมื่อเกิดการละเมิดและการแจ้งเตือน

การจัดสรรความรับผิดชอบ

หากเกิดเหตุละเมิด ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องแจ้งเหตุการละเมิดแก่สำนักงานโดยไม่ชักช้า (ภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุ) ยกเว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าเช่นกัน (PDPA มาตรา 37)

ข้อควรปฏิบัติ

- เมื่อองค์กรสถานศึกษาทราบถึงการละเมิด เจ้าหน้าที่คุ้มครองข้อมูลหรือสมาชิกผู้บริหารระดับสูงควรเป็นผู้ที่ได้รับมอบหมายให้เป็นผู้จัดการดูแลและตรวจสอบเกี่ยวกับเหตุการณ์ดังกล่าว
- ควรให้ผู้ที่เกี่ยวข้องทุกคนเล่าหรือเพิ่มเติมบันทึกข้อมูลเกี่ยวกับเหตุละเมิด สาเหตุการเกิด ตลอดจนความเสียหายและผลกระทบจากการละเมิด
- กรณีที่มีเหตุการณ์ใด ๆ ที่ส่งผลให้ข้อมูลส่วนบุคคลอาจมีความเสี่ยง (ไม่ว่าจะเป็นการทำรายละเอียดการติดต่อ/รายละเอียดบัญชีสูญหาย การเปิดเผยข้อมูลส่วนตัวผ่านการรับคำปรึกษาและอื่น ๆ) สถานศึกษาควรแจ้งผ่านทางสื่อสังคมออนไลน์ สื่อมวลชน หรือทางสื่อส่วนตัวให้เจ้าของข้อมูลส่วนบุคคลทราบถึงความเสี่ยงดังกล่าว และผลกระทบที่อาจเกิดขึ้นโดยรวดเร็วที่สุด
- หาก Third-Party ของสถานศึกษา (เช่น บริการทางไอทีหรือหุ้นส่วน) มีความเกี่ยวข้องกับการละเมิดในส่วนใดส่วนหนึ่ง องค์กรเหล่านี้จะต้องรายงานเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ตลอดจนรีบดำเนินการแก้ไขอย่างรวดเร็วและเกิดประโยชน์สูงสุด
- องค์กรสถานศึกษาควรแจ้งเหตุละเมิดไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอย่างรวดเร็วที่สุดเมื่อทราบรายละเอียด หรือภายในระยะเวลา 72 ชั่วโมงหลังจากแรกทราบเกี่ยวเหตุการณ์ที่เกิดขึ้น (PDPA มาตรา 37)

- เมื่อพบความผิดปกติของระบบหรือกระบวนการที่อาจก่อให้เกิดความไม่มั่นคงปลอดภัยหรือความผิดพลาด สถานศึกษาควรหยุดการใช้ข้อมูลนั้นในทันทีจนกระทั่งสาเหตุของปัญหาถูกระบุและได้รับการแก้ไข
- เมื่อทราบถึงสาเหตุของการละเมิด บุคลากร/เจ้าหน้าที่ภายในสถานศึกษาควรได้รับการแจ้งให้ทราบและได้รับการฝึกอบรมอย่างเหมาะสมเพื่อให้ความเสี่ยงที่เหตุการณ์ละเมิดจะบานปลายลดเหลือน้อยที่สุด
- หากการละเมิดเกิดเนื่องมาจากการดำเนินการที่ไม่ถูกต้องหรือไม่สอดคล้องตามกฎหมายขององค์กร Third-Party สถานศึกษาควรใช้อำนาจตามสัญญาข้อตกลงการประมวลผลข้อมูลลงโทษองค์กรดังกล่าว หากเกิดความเสียหายต่อกิจกรรมหรือชื่อเสียงของสถานศึกษา ตลอดจนความยุ่งยากกังวลใจใด ๆ ที่เกิดขึ้นต่อบุคลากร นักเรียน หรือพ่อแม่ผู้ปกครอง
- กรณีการละเมิดเกิดขึ้นจากความผิดพลาดในการจัดการข้อมูลส่วนบุคคลของบุคลากรหรือนักเรียนภายในองค์กร สถานศึกษาควรวางมาตรการลงโทษทางวินัยต่อผู้เกี่ยวข้องอย่างเหมาะสม และสร้างการตระหนักรู้เกี่ยวกับระเบียบนี้เพื่อป้องกันไม่ให้เกิดเหตุการณ์แบบนี้ซ้ำขึ้นอีก
- การสื่อสารขององค์กรสถานศึกษาที่เกี่ยวข้องกับเหตุละเมิดข้อมูลควรกำกับดูแลและจัดการโดยเจ้าหน้าที่คุ้มครองข้อมูลหรือผู้บริหารระดับอาวุโส เพื่อลดการสื่อสารที่อาจผิดพลาดและสร้างความเชื่อมั่น ลดความเสี่ยงด้านความกังวลใจของผู้ปกครองและนักเรียนที่มีส่วนเกี่ยวข้อง

ข้อควรหลีกเลี่ยง

- หลีกเลี่ยงการปกปิดข้อมูลเกี่ยวกับเหตุการณ์ละเมิด หากบุคลากรท่านใดมีคำถามหรือข้อสังสัยควรติดต่อเจ้าหน้าที่คุ้มครองข้อมูลหรือผู้บริหารระดับอาวุโสที่ได้รับมอบหมายให้เป็นผู้จัดการกับเหตุละเมิด
- เวลาคือปัจจัยสำคัญ สถานศึกษาไม่ควรปล่อยให้กระบวนการแจ้งเตือนผู้ที่เกี่ยวข้องล่าช้าต่อทั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและนักเรียนหรือผู้ปกครองในฐานะเจ้าของข้อมูลส่วนบุคคล

กรณีที่ 10: การขอใช้ “สิทธิเข้าถึงข้อมูลส่วนบุคคล” ของเจ้าของข้อมูล

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล (PDPA มาตรา 30) โดยบุคคลใดก็ตามที่ต้องการใช้สิทธิตามข้อกฎหมายดังกล่าวจะต้องส่ง “คำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล” ไปยังผู้ควบคุมข้อมูล แม้ไม่มีแบบฟอร์มอย่างเป็นทางการแต่คำขอดังกล่าวจะต้องมีลักษณะคือ 1.) คำขอต้องอยู่ในรูปแบบงานเขียนที่เป็นลายลักษณ์อักษร และ 2.) คำขอต้องมีข้อมูลยืนยันตัวตนของผู้ขอใช้สิทธิอย่างเพียงพอ

ข้อควรปฏิบัติ

- องค์กรสถานศึกษาควรดำเนินการยืนยันตัวตนของผู้ขอใช้สิทธิอย่างรวดเร็วที่สุดหลังได้รับคำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล และไม่ควรมีข้อมูลใดที่ถูกค้นหาหรือตรวจสอบก่อนหน้าการยืนยันตัวตน
- สถานศึกษามีเวลาตอบสนองต่อสูงสุดภายใน 1 เดือนนับตั้งแต่ได้รับคำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล อย่างไรก็ตาม องค์กรอาจพยายามตอบสนองต่อคำขอภายในระยะเวลาสั้นที่สุดเท่าที่ทำได้
- สถานศึกษาควรมอบหมายบุคลากรให้เป็นผู้ประสานงานในการค้นหารวบรวมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้ขอใช้สิทธิ โดยควรเริ่มดำเนินการค้นหาและรวบรวมข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลอย่างชัดเจนอย่างรวดเร็วที่สุด
- กรณีที่องค์กร Third-Party เป็นผู้จัดเก็บบันทึกข้อมูล บุคลากรที่ได้รับมอบหมายให้ประสานงานของสถานศึกษาควรติดต่อดูแลให้องค์กร Third-Party เหล่านี้ค้นหาเฉพาะข้อมูลที่เกี่ยวข้องและสอดคล้องกับเจ้าของข้อมูลผู้ขอใช้สิทธิเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล
- เอกสารบางตัวที่อาจพาดพิงเกี่ยวข้องกับบุคคลอื่นนอกเหนือจากผู้ขอใช้สิทธิเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล ควรได้รับการแก้ไขให้เหลือเพียงแต่ข้อมูลของผู้ใช้สิทธิฯ เท่านั้นที่สามารถอ่านเข้าใจได้
- เมื่อเสร็จสิ้นกระบวนการค้นหาข้อมูลส่วนบุคคล สำเนาของข้อมูลชุดดังกล่าวควรถูกปริ้นออกมาในรูปแบบเอกสารกระดาษและจัดส่งไปยังผู้ขอให้สิทธิฯ ผ่านไปรษณีย์แบบลงทะเบียน เพื่อให้มีหลักฐานยืนยันการนำส่งเอกสารของสถานศึกษา
- องค์กรสถานศึกษาเองควรมีสำเนาของเอกสารฉบับเต็มที่ส่งไปยังผู้ขอใช้สิทธิเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล สำรองเอาไว้ เผื่อกรณีเกิดข้อพิพาทเกี่ยวกับเนื้อหาหรือขอบเขตของเนื้อหาของเอกสารฉบับนี้ตามมาภายหลัง
- สถานศึกษาอาจปฏิเสธคำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล ในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล หรือการเข้าถึงหรือขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อที่ก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น (PDPA มาตรา 30)

ข้อควรหลีกเลี่ยง

- องค์กรสถานศึกษาไม่อาจคิดค่าบริการจากการตอบรับคำขอใช้สิทธิเข้าถึง/รับสำเนาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ เว้นเสียแต่เป็นคำขอสำเนาของเอกสารเดิมซ้ำ ๆ (สามารถคิดค่าบริการอย่างสมเหตุสมผล)
- ข้อมูล/เอกสารต้นฉบับที่เก็บรักษาโดยองค์กรไม่ควรถูกเปิดเผยเป็นส่วนหนึ่งของการตอบสนองต่อคำขอใช้สิทธิเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล
- สถานศึกษาไม่จำเป็นต้องค้นหาข้อมูลที่อยู่ในระบบ Back-up เนื่องจากไม่มีพันธะตามกฎหมายให้จัดทำสำเนาเฉพาะข้อมูลที่กำลังอยู่ในระบบการเก็บรักษาข้อมูลขององค์กรในขณะนั้น

PDPA Thailand

เราคือผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลภายใต้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีบริการหลากหลายที่ตอบโจทย์องค์กรทุกกลุ่ม

www.pdpa.online.th, www.pdpathailand.com

Our PDPA Services

- **PDPA Thailand Starter kit (New Arrival)**
  ชุดพื้นฐานรวม 8 สินค้า/บริการ “ถูกต้อง-ครบถ้วน-ปลอดภัย-คุ้มค่า” สำหรับองค์กรเริ่มต้นดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- **PDPA Consultant**
  บริการที่ปรึกษาโดยผู้เชี่ยวชาญ PDPA พร้อมเป็นผู้ช่วยเปลี่ยนแปลงขององค์กรคุณทุกย่างก้าว ให้มีการดำเนินงานที่สอดคล้องตามกฎหมายฯ

- **PDPA Compliance Audit**
  สอบทานการดำเนินงานขององค์กรเกี่ยวกับเอกสารและการบริหารจัดการข้อมูลส่วนบุคคล เสริมความมั่นใจจาก 0 เป็น 100 ว่าถูกต้องตามกฎหมาย ลดความเสี่ยงละเมิดและโทษ

- **PDPA In-House Training**
  บริการอบรมภายในด้วยหลักสูตรบรรยาย และ workshop ที่ออกแบบเฉพาะองค์กรของคุณ โดยผู้เชี่ยวชาญจาก สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

- **PDPA Public Training**
  จัดอบรมและ Workshop กฎหมาย PDPA อย่างเจาะลึก ผู้เรียนสามารถนำความรู้ไปปรับใช้ในดำเนินงานภายใต้กฎหมายได้อย่างถูกต้อง ครบทุกมิติ

- **Certification**
  ทดสอบเพื่อรับวุฒิบัตรด้านการคุ้มครองข้อมูลส่วนบุคคลมาตรฐานสากล ICDL, DCT, DDTI

จัดทำโดย

www.pdpa.online.th, www.pdpathailand.com

pdpa@digitalbusinessconsult.asia

PDPA Thailand, PDPA Thailand Starter Kit

@pdpathailand 02-029-0707