PERSONAL DATA PROTECTION GUIDELINE ประจำปี 2566

คู่มือสำหรับเตรียมความพร้อม PDPA (ฉบับสถานศึกษา)

โรงเรียนหนองโนประชาสรรค์
อำเภอกระนวน จังหวัดขอนแก่น

สารบัญ

คำนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) ประกาศลงในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 ส่งผลให้เกิดความตื่นตัวในแทบทุกวงการ ไม่เว้นแม้แต่“วงการการศึกษา”โดยกฎหมายฉบับนี้มีผลกระทบต่อการเก็บรวบรวม ใช้และเปิดเผย (การประมวลผล) ข้อมูลส่วนบุคคลในสถานศึกษา ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลหลากหลายบทบาทหน้าที่ ไม่ว่าจะเป็นบุคลากร นักเรียน พ่อแม่ผู้ปกครอง ตลอดจนผู้กเกี่ยวข้องกลุ่มอื่นสถานศึกษาเป็น “ผู้ควบคุมข้อมูล” (Data Controller) หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช่ หรือเปิดเผยข้อมูลส่วนบุคคล (PDPA มาตรา 6) จึงมีภาระหน้าที่ตามบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคล จำเป็นต้องศึกษา ว่างแผน และดำเนินการให้มีมาตรฐานและมาตรการคุ้มครองข้ออมูลส่วนบุคคลที่เหมาะสมคู่มือเตรียมความพร้อมสำหรับ PDPA (ฉบับสถานศึกษา) เล่มนี้ จัดทำขึ้นเพื่อแน่นำแน่วทางการดำเนินงาน เพื่อคุ้มครองข้อมูลส่วนบุคคลขององค์กรสถานศึกษาที่มีความซับซ้อน โดยมีประเด็นหลักๆ ที่ควรให้ความสำคัญ มากถึง 10 ประการ ด้วยหวังเป็นอย่างยิ่งว่า เอกสารฉบับนี้จะเป็นประโยชน์แก่ผู้อ่านในวงการการศึกษาและผู้ที่สนใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในบริบทของสถานศึกษา *เนื้อหาบางส่วนอ้างอิงตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) เนื่องจากเป็นกฎหมายของแม่แบบ PDPA ที่มีบังคับใช้มาเป็นระยะเวลาหนึ่ง และมีข้อบังคับเพิ่มเติมจากหน่วยงานคุ้มครอง ข้อมูลส่วนบุคคลที่ครอบคลุม หากมีข้อผิดพลาดหรือไม่สมบูรณ์ประการใด ทางสถาบันฯ ต้องขออภัยมา ณ ที่นี้

PDPA Thailand บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัดสถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

การดำเนินงานในองค์กรที่เป็นสถานศึกษาเพื่อคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) มีประเด็นหลักที่ควรให้ความสำคัญ ดังนี้

กรณีที่ 1: การติดต่อสื่อสารกับผู้ปกครอง นักเรียน หรือบุคลากร การจัดสรรความรับผิดชอบบุคลากร/

เจ้าหนาที่ระดับสูงของสถานศึกษาควรเป็ผู้รับผิดชอบในการบริหารจัดการเกี่ยวกับการติดต่อสื่อสารใดๆที่ถูกส่งออกไปในนามขององค์กร (ไม่ว่าจะเป็นการใช้กระดาษหรือเอกสารสั่งทำเฉพาะที่มีตราสัญลักษณ์หรือสามารถระบุตัวตนขององค์กรในฐานะผู้ส่งด้วยวธีการอื่น) ซึ่งไม่ได้หมายความว่าสถานศึกษาควรจัดให้มีบุคคลเพียงคนเดียวที่เป็นผู้ส่งสารทางการทั้งหมดขององค์กร อย่างไรก็ตาม ผู้ที่ส่งสารในนามขององค์กรทุกคนควรทราบว่า ในการติดต่อสื่อสารกับผู้ปกครอง นักเรียน หรือบุคลากร ซึ่งมีการใช้ข้อมูลส่วนบุคคลจะต้องดำเนินอย่างสอดคล้องตาม PDPA ข้อความบริการ vs ข้อความการตลาด

สถานศึกษาสามารถบ่งบอกคว่ามแต่กต่างระหว่าง “ข้อความบริการ” และ “ข้อความการตลาด” ได้โดย

1. “ข้อความบริการ” คือ การสื่อสารที่จำเป็นเกี่ยวกับการจัดการภารกิจในแต่ละวันของสถานศึกษา ซึ่งผู้ปกครองและนักเรียนคาดหวังว่าจะได้รับเป็นปกติอยู่แล้ว (เช่น การแจ้งเตือนเกี่ยวกับการสอบ กำหนดการเปิด-ปิดรับลงทะเบียน การเปลี่ยนแปลงวันหรือเวลานัดหมายประชุมผู้ปกครอง วันเปด ทำการของสถานศึกษาที่กำลังจะมาถึงเป็นต้น)

2. “ข้อความการตลาด” คือ การสื่อสารเชิงส่งเสรมการตลาด ซึ่งสถานศึกษาส่งถึงผู้ปกครอง/นักเรียน เพื่อโปรโมต หรือโฆษณาผลิตภัณฑ์ บริการ หรือบัตรสำหรับเขาชมงานของสถานศึกษา เป็นต้น หากมีการแจ้งให้นักเรียนและผู้ปกครองทราบตั้งแต่ชวงของการลงทะเบียนเขาสถานศึกษาแล้วการสื่อสาร

ข้อความบริการสามารถกระทำได้โดยไม่จำเป็นต้องได้รับความยินยอมล่วงหน้า

อย่างไรก็ตามด้านข้อความการตลาด GDPR บัญญัติไว้ว่า สถานศึกษาจะต้องได้รับความยินยอม ลวงหนาที่มี

ลักษณะชัดแจ้ง และให้โดยไม่ต้องมีสิงต่อบแทนจากบุคลากรและ/หรือผู้ปกครอง ก่อนการส่งสาร อิเล็กทรอนิกส์เพื่อวัตถุประสงค์ทางการตลาด ตามที่อธิบายไว้ข้างต้น ซึ่งสอดคล้องกับพระราชบัญญัติคุมครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เช่นเดียวกัน

ข้อควรปฏิบัติ

สำหรับการสื่อสารทางไปรษณีย์ สถานศึกษา/องค์กรกรควรมีหัวจดหมายทางการ และอนุญาตเฉพาะ บุคลากร/เจ้าหนาที่ที่เกี่ยวของเทานั้นที่สามารถเขาถึงทรัพยากรนี้ เพื่อควบคุมจำนวนของผู้ที่เป็น ตัวแทนขององค์กรสื่อสาร ในฐานะตัวแทนขององค์กร

ผู้ที่ส่งสารในนามขององค์กรควรดำเนินการให้แน่ใจว่า ครูใหญ่/ผู้อำนวยการ/ผู้บริหารองค์กรกรรับรู้ และให้การอนุมัติเห็นด้วยก่อนการสื่อสารออกไปในทุกๆ ครั้งผู้ที่ได้รับมอบหมายให้เป็นผู้ส่งสารการตลาดทางตรงหรือโปรโมชั่นรูปแบบอิเล็กทรอนิกส์ ไม่ว่าจะเป็น ผ่านทางอีเมล SMS หรือโซเชียลมีเดีย ควรดำเนินการให้แน่ใจว่าได้รับความยินยอมจากผู้ที่คาดว่าเป็น ผู้รับสารล่วงหน้า โดยความยินยอมจะต้องให้โดย “ระบุวัตถุประสงค์ชัดเจนอย่างไรข้อกำกวม และเจ้าของข้อมูลสามารถเลือกได้อย่างอิสระ”ข้อความสื่อสารการตลาดทางตรงหรือโปรโมชั่น จะต้องมีตัวเลือกหรือฟังกชันให้ “ถอนความยินยอม” เพื่อปฏิเสธการรับสารลักษณะดังกล่าวอีกในอนาคตการสื่อสารใดๆ ในนามขององค์กร ควรระบุรายละเอียดติดต่อของผู้ส่งหรือสมาชิกในทีมคนอื่นๆ ด้วย ในกรณีที่ผู้รับสารต้องการความชัดเจนหรือติดตามผลสถานศึกษาควรเน้นย้ำความถูกต้องและการข้อความยินยอมในการใช้ข้อมูลรายละเอียด การติดต่อของสมาชิกโรงเรียน ณ จุดลงทะเบียน – รวมถึงข้อมูลของผู้ปกครองที่อาจได้รับการติดต่อไปในกรณีของเด็กนักเรียนที่ยังไม่บรรลุนิติภาวะการส่งข้อคว่ามบริการผ่านทางกรุ๊ปบนโซเชียลมีเดียหรือแอปพลิเคชันแชท ต้องคำนึงและควบคุม ให้เนื้อหาสารที่ส่งออกไปมีความสอดคล้องกับวัตถุประส่งคของการก่อตั้งกลุ่มนั้น ซึ่งตรงกับบัญญัติ ของ PDPA ที่ว่า ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประส่งคที่ได้แจ้งเจ้าของข้อมูลไว้ก่อนหรือในขณะที่เก็บรวบรวม (PDPA มาตรา 21) อีเมลทางการขององค์กรกรที่ถูกส่งหาผู้รับหลายคนในครั้งเดียว จะต้องใช้ฟังก์ชัน BCC (Blind Carbon Copy) เสมอ เพื่อป้องกันไม่ให้ข้อมูลที่อยูอีเมล์ของผู้รับถูกเปิดเผยต่อคนอื่นๆ โดยไม่จำเป็น

สถานศึกษา ควรตระหนักว่าในบางกรณีครอบครัวหรือผู้ปกครองของนักเรียนอาจอยู่ในสถานะหย่าร้างหรือแยกกันอยู่ องค์กรควรมีมาตรการเพื่อให้แน่ใจว่าครอบครัวหรือผู้ปกครองทั้ง 2 ท่าน ได้รับการติดต่อ/ข้อมูลข่าวสารที่เกี่ยวของกับลูก (ยกเว้นมีการตกลงกัน) ตามหลักการของ PDPA ที่ระบุว่า ผู้ควบคุมข้อมูลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด (PDPA มาตรา 35) ข้อความบริการที่เกี่ยวข้องกับกิจกรรมของนักเรียนที่ยังไม่บรรลุนิติภาวะ (อายุต่ำกว่า 20 ปีบริบูรณ์) โดยเฉพาะนักเรียนที่มีอายุไม่เกิน 10 ปี ควรแจ้งไปยังผู้ปกครองที่มีอำนาจกระทำการ แทนนักเรียน เหล่านั้น แทนที่จะดำเนินการผ่านนักเรียนโดยตรงขอควรหลีกเลี่ยงสถานศึกษา ควรงดเว้นการส่งโปรโมชั่น การระดมเงินทุน และข้อความทางการตลาดไปยังบุคคลที่มีอายุต่ำกว่า 20 ปี บริบูรณ์ การส่งข้อความ ยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (PDPA มาตรา 19) สถานศึกษาจึงไม่ควรใช้งาน “กล้องตัวเลือกที่คลิกเลือกตั้งต้นให้อัตโนมัติ (Pre-ticked)” ในแบบฟอร์มการสมัครหรือลงทะเบียน

กรณีที่ 2: การลงทะเบียนเข้าร่วมกิจกรรม การจัดสรรความรับผิดชอบ

ครูใหญ่/ผู้อำนวยการ/ผู้บริหารองค์กร และเลขานุการ ควรเป็นผู้รับผิดชอบหลักในการบริหารจัดการและดำเนินกระบวนการ ลงทะเบียนใดๆ ภายในสถานศึกษา หัวหน้าชั้นและบุคลากรคนอื่นๆ อาจเป็นผู้เก็บรวบรวมข้อมูลโดยตรงจากนักเรียน และผู้ปกครองอย่างไรก็ตาม กระบวนการโดยรวมยังคงเป็นความรับผิดชอบของสถาบันการศึกษาในฐานะนิติบุคคลและผู้ควบคุมข้อมูลด้านการจัดการแบบฟอรีมสำหรับสมัครหรือลงทะเบียนควรออกแบบให้ได้รับข้อมูลครบถ้วนจากนักเรียนและผู้ปกครอง (ในกรณีที่นักเรียนยังไม่บรรลุนิติภาวะ) เพื่อให้ตรงตามวัตถุประส่งคขององค์กรกร ขณะเดียวกันก็ควรเก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นเพื่อให้สอดคล้องกัน

<u>ข้อควรปฏิบัติ</u>

ออกแบบแบบฟอร์มการสมัคร/ลงทะเบียนให้มีช่องสำหรับกรอกข้อมูล (เท่าที่จำเป็น) เพื่อตอบสนองต่อวัตถุประสงค์การเก็บข้อมูลอย่างครบถ้วนระบุรายละเอียดติดต่อของเจ้าหนาที่คุมครองข้อมูล (DPO) หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในช่วงของแบบฟอร์มที่เห็นว่ามีความเหมาะสม เพื่อให้ผู้ที่สมัครหรือลงทะเบียนสามารถติดต่อองค์กรกรได้ในกรณีที่ต้องการความกระจ่างชัดแนะนำให้องค์กรกรแต่งตั้งเจ้าหน้าที่คุมครองข้อมูลส่วนบุคคล เพื่อเป็นผู้รับผิดชอบในการตรวจสอบการดำเนินงานของสถานศึกษาในการการเก็บรวบรวม การจัดการข้อมูลของเจ้าของข้อมูลส่วนบุคคล และให้คำแนะนำที่อาจเป็นประโยชน์ต่อการประมวลผลข้อมูลดังกล่าว แม้สถานศึกษาไม่ได้เป็นองค์กรกรที่ถูกกำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลตามที่ระบุไว้ในกฎหมายคุมครองข้อมูลส่วนบุคคล (PDPA มาตรา 41) ก็ตามหากสถานศึกษาของคุณเป็นเครือธุรกิจหรือเครือกิจการเดียวกัน อาจแต่งตั้ง “เจ้าหนาที่คุ้มครอง ข้อมูลส่วนบุคคลรวม” เป็นบุคคลหรือคณะบุคคลเดียวกันได้โดยต้องติดต่อเจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคลได้โดยง่าย ณ จุดลงทะเบียน (หรือหน้าเข้าลงทะเบียนในกรณีออนไลน์) นักเรียนและวัตถุประสงค์ดังกล่าวผู้ปกครองจะต้องได้รับการบอกกล่าวว่าข้อมูลส่วนบุคคลของพวกเขาจะถูกนำไปใช้งานภายใต้วัตถุประสงค์ใดหากมีพื้นที่เพียงพอ คุณควรเขียนบรรยายสั้นๆ ในแต่ละส่วนของแบบฟอร์มลงทะเบียนเพื่ออธิบาย ถึงเหตุผลว่าทำไมข้อมูลนั้นๆ จึงต้องถูกเก็บรวบรวม พร้อมระบุถึงกระบวนการใช้งานและเปิดเผยข้อมูล เพื่อสร้างความเข้าใจและความคาดหวังที่เป็นเหตุเป็นผลของผู้กรอกแบบฟอรม์ กรณีนักเรียนที่ยังไม่บรรลุนิติภาวะแบบฟอร์มลงทะเบียนควรมีส่วนที่แยกออกมาอย่างชัดเจนสำหรับ ผู้ปกครองโดยเฉพาะ สำหรับการ“เลือกรับ” ข้อมูลเกี่ยวกับโปรโมชั่นและกิจกรรมระดมทุนต่างๆ โดยจะต้องให้ผู้ให้ความยินยอมทำเครื่องหมายหรือคลิกยอมรับเองอย่างอิสระ (ไม่สามารถใช้กล้อง ที่ทำเครื่องหมายให้ล่วงหน้าได้) ซึ่งหากผู้ปกครองไม่ให้ความยินยอม องค์กรควรมีมาตรการให้แน่ใจว่าทันทีที่กรอกและส่งมอบเรียบร้อยสถานศึกษาควรเรียบเรียงและนำส่งแบบฟอร์มทั้งหมดไปยังสถานที่เก็บรักษากลางขององค์กรอย่างรวดเร็วที่สุดและหากเป็นไปได้ก็ควรพยายามลดการเก็บข้อมูลในรูปแบบเอกสารกระดาษให้ได้มากที่สุดด้วยเช่นกันโดยอาจแปลงและย้ายข้อมูลจากเอกสารแบบฟอร์มกระดาษที่นักเรียนและผู้ปกครองกรอกเข้ามาเข้าสู่ระบบคอมพิวเตอร์

เนื่องจากมีความปลอดภัย และ ประสิทธิภาพที่สูงกว่าในแง่ของการจัดเก็บ การจัดการ การประมวลผล และการเรียกข้อมูลเพื่อใช้งานหากมีการแปลงข้อมูลจาก Hard-copy เป็นเอกสารอิเล็กทรอนิกสแล้ว เอกสาร Hard-copy ดังกลาวนั้นควรมีมาตรการในการเก็บรักษาอย่างปลอดภัยหรือดำเนินการทำลายตามความเหมาะสม โดยสถานศึกษาควรปรับปรุงนโยบายการจัดการกับข้อมูลที่เกิดขึ้นในลักษณะนี้ เพื่อกระตุ้นให้เกิดแนวปฏิบัติ ที่ดีองค์กรกรจะต้องไม่ขอข้อมูลมากเกินความจำเป็น นอกเหนือจากที่ต้องการจากนักเรียนหรือผู้ปกครอง (หรือผู้ปกครองที่ใช้อำนาจแทนนักเรียน) ผ่านแบบฟอร์มสมัคร/ลงทะเบียน หากยังไม่มีความจำเป็นในการ ประมวลผลข้อมูลนั้นการจัดทำแบบฟอร์ม ไม่ควรเขียนกำกับชองว่างสำหรับกรอกข้อมูลใดๆ ว่า “จำเป็น” นอกเหนือจากเป็นข้อบังคับในระยะยาวข้อควรหลีกเลี่ยงบุคคลเหลานี้ ทางการหรือข้อบังคับตามบทกฎหมาย ซึ่งหากมีการระบุฯ ก็ควรอธิบายถึงข้อกำหนดของกฎหมายที่เกี่ยวของกับข้อมูลดังกล้าวนั้นประกอบด้วยองค์กรกรสถานศึกษาจะต้องไม่อนุมานเอาเองว่าผู้ปกครองหรือบุคลากรจะอยากได้รับข่าวสารทางด้าน การตลาดหรือโปรโมชั่น เพียงเพราะพวกเขาเกี่ยวของกับองค์กรกรหรือมีบุตรเรียนอยู่ที่สถานศึกษานั้นๆ แบบฟอร์ม ข้อประมวลผล ข้อมูลเพื่อวัตถุประสงค์ทางการตลาดจากบุคคลเหลานี้จะต้องให้พวกเขาเป็นผู้ “เลือกรับ (Opt-in)” ข่าวสารอย่างอิสระด้วยตนเอง เช่นเดียวกับบุคคลอื่นๆ (ไม่ใชตัวเลือกที่จะปฏิเสธ ที่จะไม่รับข่าวสาร (Opt-out)) จะไม่ได้รับการติดต่อด้วยเหตุผลดังกล่าว

กรณีที่ 3: การขอให้เปิดเผยข้อมูลส่วนบุคคล

การจัดสรรความรับผิดชอบหลายครั้งหลายคราว สถานศึกษาอาจจำเป็นต้องให้หรือเปิดเผยข้อมูลของบุคลากรหรือนักเรียน ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 27 กำหนดไว้ว่าห้ามมิให้องค์กรเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องข้อความยินยอมตามที่กฎหมายกำหนด ดังนั้น เมื่อตกอยู่ในสถานะที่จะต้องเปิดเผยข้อมูล ส่วนบุคคลตามคำขอดังกล่าว องค์กรจะต้องแสดงความรับผิดชอบในฐานะผู้ควบคุมข้อมูลและจัดวางมาตรการสำหรับการขอเปิดเผยข้อมูลส่วนบุคคลที่เหมาะสม โดยจะสามารถเปิดเผยข้อมูลตามคำขอได้หากสถานศึกษา ได้พิสูจน์แล้วว่าคำขอนั้นสามารถกระทำได้มีความเหมาะสม ข้อควรปฏิบัติผู้อำนวยการ ผู้บริหารระดับสูง หรือบุคลากรของสถานศึกษาที่ได้รับมอบหมายให้รับผิดชอบตอบสนองต่อคำขอประเภทนี้ ควรเป็นผู้ที่สามารถพิจารณาได้ว่า คำขอเพื่อจะเปิดเผยข้อมูลส่วนบุคคลที่เก็บ รักษาโดยองค์กรนั้น จะต้องข้อความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือได้รับยกเวนไม่ต้องขอความยินยอมตามที่กฎหมายกำหนดหรือไม่แม้ว่าคำขอให้เปิดเผยข้อมูลดังกล่าวจะสามารถกระทำได้ตามกฎหมายสถานศึกษาควรเปิดเผย ข้อมูลน้อยที่สุดเท่าที่จำเป็น เพื่อดำเนินการตามคำขอเท่านั้นบุคลากรของสถานศึกษาควรทราบเกี่ยวกับข้อกฎหมาย หรือภาระผูกพันตามกฎหมายที่อาจนำมาใช้อนุญาตให้องค์กรกรเปิดเผยข้อมูลส่วนบุคคลของนักเรียนได้ในการดำเนิน

<u>ข้อควรหลีกเลี่ยง</u>

ข้อมูลส่วนบุคคลของบุคลากรหรือนักเรียนไม่ควรสามารถเขาถึงได้โดยทั่วไปข้อมูลส่วนบุคคลที่เกี่ยวของกับการให้คำปรึกษาหรือการสนับสนุนของสถาบันไม่ควรถูกเปิดเผย นอกเสียจากได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล (หรือผู้ปกครองในกรณีเป็นผู้เยาว์) หรือได้รับอนุญาตตามอำนาจทางกฎหมายองค์กรกรสถานศึกษาไม่ควรเปิดเผยข้อมูลส่วนบุคคลนอกเสียจากได้รับแบบฟอร์มคำขออย่างเป็นลายลักษณ์อักษรองค์กรกรสถานศึกษาไม่ควรเปิดเผยข้อมูลส่วนบุคคลของบุคลากร นักเรียน หรือผู้ปกครอง ไม่ว่าจะเป็นรายบุคคลหรือหลายๆ คนพร้อมกันให้กับองค์กรอื่น เว้นแต่เป็นการปฏิบัติตามกิจการตามปกติ

กรณีที่ 4: การจัดการความยินยอม การจัดสรรความรับผิดชอบ

กฎหมายคุมครองข้อมูลส่วนบุคคลอย่าง PDPA การประมวลผล (เก็บรวบรวม ใช่และเปิดเผย) ข้อมูลส่วนบุคคลกระทำได้โดยชอบหากองค์กรกรสามารถอ้างอิงฐานทางกฎหมายสำหรับการประมวลผลข้อมูลนั้นๆ โดย “ความยินยอม” เป็น 1 ใน 7 ฐานการประมวลผลข้อมูลสถานศึกษาจำเป็นต้องได้รับความยินยอมเพื่อประมวลผลข้อมูลโดยชอบตามกฎหมาย หากไม่สามารถอ้างฐานการประมวลผลอื่นมารองรับได้ โดยในบริบทของสถานศึกษา อาจจำเป็นต้องขอความยินยอมจากนักเรียนซึ่งมีสถานะเป็นผู้เยาว์ โดยการข้อความยินยอมจากผู้เยาว์ที่ยังไม่บรรลุนิติภาวะให้ดำเนินการดังนี้ (PDPA มาตรา 20) ผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมาย ให้ข้อความยินยอมจากตัวผู้เยาว์เอง และจากพ่อแม่ ผู้ปกครองร่วมด้วย ผู้เยาว์อายุไม่เกิน 10 ปี ให้ภายใต้ PDPA ข้อความยินยอมต้องกระทำโดยชัดแจ้ง เป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์โดยต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย และต้องแยกส่วนออกจาก ข้อความอื่นอย่างชัดเจนมีรูปแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย ไม่หลอกลวงหรือ ทำให้เจ้าของข้อมูลเขาใจผิดในวัตถุ ประสงค์ นอกจากนั้นต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (PDPA มาตรา 19) หากการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลของสถานศึกษา ไม่เป็นไปตามที่กำหนดไว้ข้างต้น ก็จะไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และสถานศึกษาไม่อาจดำเนินการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ข้อความยินยอม

<u>ข้อควรปฏิบัติ</u>

สถานศึกษาควรบอกกล่าวแนะนำพ่อแม่ ผู้ปกครองและตัวนักเรียนเอง เกี่ยวกับกิจกรรมหรือบริการ (เช่น การให้คำปรึกษาของโรงเรียน) ที่มีการข้อความยินยอมเกิดขึ้นเมื่อเปิดรับสมัครหรือลงทะเบียน

แบบฟอร์มหรือเอกสารใดๆ ที่กรอกโดยนักเรียนและ/หรือพ่อแม่ผู้ปกครอง ควรถูกเก็บรักษาในแฟ้มข้อมูลที่เกี่ยวของกับนักเรียนเป็นรายบุคคล พร้อมจัดให้มีมาตรการรักษาความมั่นคง ปลอดภัย ที่เหมาะสม เพื่อเป็นการคุ้มครองข้อมูลและรักษาความลับของเจ้าของข้อมูลและผู้เกี่ยวข้อง

การให้ความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล ก่อนวันที่ พ.ร.บ.คุมครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้บังคับ สถานศึกษาสามารถเก็บรวบรวมและใช้ข้อมูลดังกล่าวต่อไปได้ ทั้งนี้ สถานศึกษาควรกำหนดวิธีการยกเลิกความยินยอม และประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลไม่ว่าจะเป็นบุคลากร นักเรียน หรือผู้ปกครอง ที่ไม่ประสงค์ให้สถานศึกษาเก็บรวบรวมหรือใช้ข้อมูลดังกล่าว และสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

<u>ข้อควรหลีกเลี่ยง</u>

สถานศึกษาควรพิจารณาการใช้ฐานกฎหมายในการประมวลผลข้อมูล หากไม่สามารถใชฐานทางกฎหมายอื่นๆ ที่กฎหมายกำหนดในการเก็บรวบรวมข้อมูล จงจะพิจารณาใช้การเก็บรวบรวมด้วยฐานความยินยอม

ความยินยอมต่อกิจกรรมหรือบริการหนึ่ง ไม่อาจนำมาคาดเดาเหมารวมว่าเจ้าของข้อมูลส่วนบุคคล จะให้ความยินยอมต่อบริการอื่นๆ ที่มีความคล้ายคลึงกันได้ หากองค์กรกรสถานศึกษาต้องการนำเสนอ กิจกรรมหรือบริการอื่น ๆ จะต้องจัดทำแบบฟอร์มขอความยินยอมแยกออกจากกันอย่างชัดเจนพ่อแม่ ผู้ปกครอง ผู้มีอำนาจกระทำการแทนผู้เยาว์เท่านั้น

กรณีที่ 5: การเก็บรักษาบันทึกข้อมูลและการลบทำลาย การจัดสรรความรับผิดชอบ

สถานศึกษาจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลบางประเภทเอาไว้เป็นระยะเวลาที่แตก่ตางกัน ด้วยเหตุผล เช่น เพื่อให้บริการด้านการลงทะเบียนและธุรการ เพื่อปฏิบัติตามกฎเกณฑ์หรือกฎหมาย หรือเพื่อเก็บรักษา บันทึกประวัติของทางองค์กร เป็นต้น โดยสถานศึกษาจะต้องพยายามหาสมดุลระหว่างการเก็บรักษาข้อมูลเพื่อประโยชนขององค์กร และการลด ความเสี่ยงด้านข้อมูล ด้วยเทคโนโลยีการจัดเก็บแบบอิเล็กทรอนิกสในปจจบันนี้ องค์กรกรสามารถจัดเก็บข้อมูลได้อย่างยาวนาน ด้วยคาใชจายที่ต่ำ ส่วนบันทึกเอกสารกระดาษอาจใชพ้นที่มากและอาจเป็นภาระที่นารำคาญหากไม่ได้ดำเนินการ จัดระเบียบอย่างเหมาะสม มีประสิทธิภาพ และมีคว่ามมั่นคงปลอดภัย

หลักสำคัญหนึ่งของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง PDPA ก็คือ องค์กรกรควรเก็บรักษาข้อมูล เอาไว้เป็นระยะเวลาเพียงเท่าที่จำเป็นภายใต้รูปแบบที่สามารถระบุตัวต้นของบุคคลได้ เพื่อบรรลุวัตถุประสงค์ด้านการดำเนินงานและตามภาระผูกพันตามกฎหมาย (เช่น งานทะเบียนธุรการสมาชิก ข้อผูกพันการประเมินผลการจ้างงานและเงินเดือน การรายงานไปยังหน่วยงานต่างๆ ของรัฐ การเก็บรักษาข้อมูลเพื่อวัตถุประสงค์ทางประกันหรือกฎหมาย ฯลฯ) เมื่อหมดความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลจะต้องถูกลบ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (PDPA มาตรา 33)การลบหรือทำลายข้อมูลที่ไม่มีความจำเป็นสำหรับการดำเนินงานขององค์กรอีกต่อไปโดยหลักกไม่เกี่ยวกับเครือข่ายทางไอทีขีดความสามารถของระบบหรือพ้นที่จัดเก็บข้อมูล ที่เหลืออยู่ขององค์กรกรสถานศึกษา แต่ประเด็นคือบันทึกข้อมูลส่วนบุคคลจะสามารถถูกลบหรือทำลายได้อย่างรวดเร็วที่สุดเมื่อใดข้อควรปฏิบัติองค์กรสถานศึกษา (และแต่ละแผนกที่เกี่ยวของกับข้อมูล) ควรทราบเกี่ยวกับข้อบังคับทางกฎหมาย เกี่ยวกับระยะเวลาการเก็บรักษา บันทึกข้อมูลทางธุรการ สวัสดิการสังคม และการเงินสถานศึกษาควรรางนโยบายการเก็บรักษาและทำลายข้อมูลและจัดทำตารางระยะเวลาการเก็บ รักษาข้อมูลส่วนบุคคลแต่ละประเภทที่กำลังถูกประมวลผลโดยองค์กร ตามข้อกำหนดทางกฎหมาย หรือแนวทางการเก็บรักษาข้อมูลของแต่ละหมวดหมู่ผู้บริหาร/ผู้จัดการ ผู้อำนวยการ หรือบุคลากรของสถานศึกษา ที่มีสิทธิ/ได้รับอนุญาตให้สามารถเข้าถึงบันทึกข้อมูลส่วนบุคคล ควรเข้าใจเกี่ยวกับนโยบายการเก็บรักษาและทำลายข้อมูล และกลุ่มคนเหล่านี้ควรดำเนินการให้แน่ใจว่าบันทึกข้อมูลนั้นๆ ถูกเก็บรักษาเอาไว้ไม่เกินระยะเวลาที่ควรจะเป็นโดยที่อ้างอิงกับนโยบาย และตารางกำหนดเวลาการเก็บรักษาสถานศึกษาต้องคำนึงเสมอว่าข้อกำหนดเกี่ยวกับระยะเวลาการเก็บรักษาข้อมูลบังคับใชกับทั้งบันทึก ข้อมูลในระบบอิเล็กทรอนิกส์และแบบเอกสารกระดาษบันทึกข้อมูลส่วนบุคคลของบุคลากร นักเรียน และผู้ปกครอง บางครั้งอาจถูกนำไปประมวลผล นอกสถานที่แต่ก็ควรถูกเก็บรวบรวมกลับมาไว้ภายในศูนยเก็บข้อมูลของสถานศึกษาโดยไม่ชักช้า เพื่อความปลอดภัยในการเก็บรักษาข้อมูลและดำเนินการลบหรือทำลายหากหมดวัตถุประสงค์ในการประมวลผลเมื่อบรรลุวัตถุประสงค์การประมวลผลขององค์กรสถานศึกษาแล้ว เอกสารใดๆ ที่มีข้อมูลส่วนบุคคลไม่ว่าจะเป็นจดหมายหรือใบกำกับภาษีเก่า แบบฟอร์มการสมัครลงทะเบียนฯลฯ ควรถูกนำไปทำลาย ให้เป็นชิ้นเล็กชิ้นน้อยก่อนจะถูกนำไปทิ้งในสถานที่ที่เหมาะสม บันทึกข้อมูลฉบับจริงสมควรถูกเก็บรักษาเอาไว้ ณ สถานที่เก็บส่วนกลางของสถานศึกษาที่มีความมั่นคงปลอดภัยมากกว่าจะกระจายอยูตามแผนกต่างๆ หรืออยู่ที่หลายบุคคลอุปกรณ์คอมพิวเตอร์ที่ถูกใช้สำหรับการประมวลผลข้อมูลโดยสถานศึกษา ควรดำเนินการตามวธี การที่เหมาะสมในการลบรองรอยตางๆ ของข้อมูล เช่น การลบข้อมูลถาวร (Formating) เป็นต้น ก่อนส่งต่อยกเลิกการใช้งาน หรือการรีไซเคิลอุปกรณ์เหล่านั้นหากต้องพึ่งพาบริการจัดการข้อมูลจากองค์กร Third-Party ในการจัดเก็บ กู้คืน หรือทำลายข้อมูล สถานศึกษาจะต้องจัดให้มีสัญญาข้อตกลงการประมวลผลข้อมูล ก่อนหน้าการใชบริการจากองค์กร ภายนอกเหล่านั้นเพื่อควบคุมการดำเนินงานตามหน้าที่ดังกล่าว

ข้อควรหลีกเลี่ยง

องค์กรจะต้องไม่เก็บรักษาบันทึกข้อมูลส่วนบุคคลเอาไว้ยาวนานเกินกว่ากำหนดการที่ตกลงกันบอร์ดบริหาร ผู้อำนวยการ และ/หรือบุคลากร ไม่ควรเก็บรักษาสำเนาบันทึกข้อมูลส่วนบุคคลของ องค์กรเอาไว้ที่บานพักอาศัยของตนเอง เมื่อบันทึกข้อมูลชุดนั้นฉบับจริงถูกลบทำลายไปแล้วตามนโยบายการเก็บรักษาและลบทำลายข้อมูล เราควรตระหนักไว้เสมอว่า สถานศึกษา/องค์กรที่มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล จะต้องเป็นผู้รับผิดชอบสูงสุดเกี่ยวกับการเก็บรวบรวม เก็บรักษา ความมั่นคงปลอดภัย และระยะเวลาการเก็บรักษาของข้อมูลส่วนบุคคล โดยไม่ควรมีบุคลากรคนใดคนหนึ่ง (ไม่ว่าประจำหรือสัญญาจ้าง) ที่ลบทำลาย หรือจัดทำข้อมูลส่วนบุคคลให้เป็นนิรนามโดยพลการเอกสารกระดาษที่มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวต่างๆ ไม่ควรแค่ถูกโยนทิ้งลงในถังขยะ แต่สมควรถูกทำลายให้เป็นชิ้นเล็กชิ้นน้อยอย่างปลอดภัยก่อนถูกทิ้งทุกครั้งอุปกรณ์คอมพิวเตอร์ซึ่งใช้ประมวลผลข้อมูลส่วนบุคคลไม่ควรถูกขายทิ้งหรือส่งไปรีไซเคิลโดยไม่ได้รับการ “ล้าง” ข้อมูลส่วนบุคคลออกจากฮาร์ดไดร์ฟโดยมืออาชีพ

กรณีที่ 6: การใช้ภาพถ่ายและวิดีโอ

ภาพถ่ายและวิดีโอสามารถบันทึกลักษณะต่างๆทางกายภาพของบุคคล จงนับเป็นข้อมูลส่วนบุคคล ที่องค์กรต้องดำเนินการคุ้มครอง/บริหารจัดการให้สอดคล้องตาม PDPA (รวมถึง GDPR หรือกฎหมาย คุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวของฉบับอื่น ๆ) การจัดสรรความรับผิดชอบสถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการบันทึกภาพหรือวิดีโอในงานกิจกรรมหรือ การแข่งขันต่างๆ ที่สถานศึกษาจัดขึ้นและดำเนินการเก็บรักษาบันทึกภาพ (Footage) ไว้นั้น สามารถดำเนินการ ภายใต้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) ของผู้ควบคุมข้อมูล โดยจะต้องมีการแจ้งถึงการเก็บภาพดังกล่าวพร้อมทั้งวัตถุประสงค์ในการเก็บภาพ ทั้งนี้ ผู้เข้าร่วม ไม่ว่าจะเป็นนักเรียน ผู้ปกครอง บุคลากร เป็นต้น ยอมมีความคาดหมาย (Expectation) ว่าจะมีการถ่ายภาพ และภาพถ่ายดังกล่าวอาจถูกนำไปใช้ได้ และควรเปิดชองให้ผู้เข้าร่วมแสดงเจตจำนงไม่ยินยอม/คัดค้านการเปิดเผยรูปดังกล่าวนั้นได้ รวมถึงสถานศึกษาจะต้องดำเนินการ เพื่อให้แน่ใจว่าการประมวลผลภาพต่างๆ ให้เป็นไปอย่างเหมาะสมและสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อควรปฏิบัติ

หากสถานศึกษาวางแผนจะเก็บภาพของกิจกรรมหรือการแข่งขันตางๆ ที่กำลังจะจัดขึ้น ผู้เข้าร่วมงานควรได้รับการแจ้งเตือนล่วงหน้าเมื่อสามารถกระทำได้ เช่น แทรกลงในโปสเตอร์หรือบัตรสำหรับ เข้างานว่า“ภายในงานจะมีการบันทึกภาพและวิดีโอ ซึ่งอาจถูกนำไปใช้โปรโมตและประชาสัมพันธเพื่อประโยชนของสถานศึกษาในอนาคต” เป็นต้น

ณ สถานที่จัดกิจกรรม แน่ะนำให้สถานศึกษามีการติดโปสเต่อรเป็นระยะ ๆ ให้สามารถสังเกตเห็นได้ เพื่อย้ำเตือนผู้เขารวมว่าจะมีการถายภาพ/วดีโอ

อาณาเขตของสถานศึกษาที่มีกลองวงจรปด CCTV ควรติดปายประกาศเตือนว่ามีการบันทึกภาพ เอาไว้ให้สามารถมองเห็นได้อย่างชัดเจน เพื่อเป็นการแจ้งให้บุคลากร ผู้ปกครอง และนักเรียนทราบ โดยระบุวัตถุประส่งค พรอมรายละเอียดติดต่อเจ้าหนาที่คุมครองข้อมูลส่วนบุคคลหรือผู้บริหารระดับ สูงขององค์กรกรที่รับผิดชอบ ในกรณีที่มีขอส่งสัยหรือคว่ามกังวลใจระบบวงจรปิด CCTV ควรได้รับการตรวจสอบดูแลอยู่เป็นประจำ เพื่อเช็กดูว่าภาพที่บันทึกได้ถูกนำ ไปใชตรงกับวัตถุประสงค์ของการติดตั้ง และเพื่อป้องกันหรือตรวจสอบกิจกรรมที่ไม่สอดคล้องกับกฎหมาย ตลอดจนการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตก่อนกิจกรรมหรือการแข่งขันใดๆ องค์กรสถานศึกษาจะต้องทำสัญญาข้อตกลงการประมวลผล ข้อมูลกับช่างภาพมืออาชีพที่จ้าง และระบุมาตรการ/มาตรฐานเกี่ยวกับการเก็บรวบรวม ใช้ และการ เก็บรักษาข้อมูลภาพถ่าย/วิดีโอที่จะเกิดขึ้นภายในงาน

ข้อควรหลีกเลี่ยง

ภาพถ่ายและวิดีโอที่ถูกถ่ายในงานกิจกรรมของสถานศึกษาไม่ควรนำไปเผยแพร่โดยปราศจากการรับรู้จากบุคคลในภาพ แม้เป็นการยากที่จะได้รับอนุญาตจากทุกคนในภาพคนกลุ่มใหญ่ๆ แต่องค์กรก็ควรพยายามทำให้พวกเขารับรู้ล่วงหน้าว่าภาพถ่ายหรือวิดีโอจะถูกโพสต์ลงบนเว็บไซต์หรือโซเชียลมีเดียของสถานศึกษา หรือแจ้งเตือนว่าภาพของพวกเขาอาจถูกนำไปใช้งานเพื่อวัตถุประสงค์ดังกล่าว บุคลากรไม่ควรสามารถเปิดหรือเข้าถึงภาพถ่ายและวิดีโอ (รวมถึงภาพจาก CCTV) อย่างไม่มีข้อจำกัด เพื่อเป็นการป้องกันและลดความเสี่ยงของการใช้ภาพอย่างไม่ได้รับอนุญาตหรือเกินวัตถุประสงค์

กรณีที่ 7: ความเกี่ยวข้องกับผู้ให้บริการ Third-Party

สถานศึกษาอาจจำเป็นต้องใช้บริการจากผู้เชี่ยวชาญเฉพาะทางภายนอกองค์กรกรซึ่งเป็นผู้ให้บริการบุคคล ที่สาม (Third-Party) เพื่อช่วยเหลือในการทำงานในหลากหลายโอกาส ยกตัวอย่างเช่น บริษัท Headhunter สรรหาบุคลากรและผู้เชี่ยวชาญ บริษัทจัดการบัญชีดูแลเงินเดือนบุคลากร สำนักงานที่ปรึกษาทางจิตวิทยา สำหรับช่วยเหลือนักเรียน หรือผู้ให้บริการด้านไอทีที่ดูแลเครือข่ายและโครงสร้างพื้นฐาน เป็นต้น องค์กร/บริษัทผู้ให้บริการบุคคลที่สามข้างต้นจะมีสิทธิ์และความสามารถเข้าถึงข้อมูลส่วนบุคคลของสถานศึกษาได้จึงถือว่าเป็น “ผู้ประมวลผลข้อมูล” สถานศึกษาจะต้องดำเนินการจัดทำ “สัญญาข้อตกลงการประมวลผลข้อมูล” ไม่ว่าในรูปแบบเอกสารกระดาษหรืออิเล็กทรอนิกส์กับบริษัทเหลานี้อย่างเป็นทางการก่อนเริ่มต้นรับบริการ (PDPA มาตรา 40) การจัดสรรความรับผิดชอบสถานศึกษาในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการจัดให้มีสัญญาข้อตกลงการประมวล ข้อมูลส่วนบุคคล ระหว่างตนกับผู้ให้บริการซึ่งมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนิน งานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามสถานศึกษาหรือทีมผู้บริหารของสถานศึกษา กำหนดและสอดคล้องตามกฎหมาย

ข้อควรปฏิบัติ

สถานศึกษาควรเช็กให้แน่ใจว่าผู้ให้บริการ Third-Party มีมาตรฐานการให้บริการที่มีความชำนาญ ไว้วางใจได้และสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) รวมถึงกฎหมาย คุ้มครองข้อมูลส่วนบุคคลฉบับอื่น ๆ ที่เกี่ยวข้องกับองค์กรสถานศึกษาจะต้องแน่ใจว่ามีสัญญาข้อตกลงการประมวลผลข้อมูลที่มีผลบังคับสมบูรณ์ ก่อนหน้าที่ผู้ให้บริการ Third-Party จะสามารถเข้าถึงข้อมูลส่วนบุคคลใดๆ ที่สถานศึกษารับผิดชอบดูแลอยู่ สัญญาข้อตกลงการประมวลผลข้อมูลควรได้รับการทบทวนเป็นประจำ อย่างน้อยปีละ 1 ครั้ง และผู้ควบคุมข้อมูลจะต้องดูแลให้แน่ใจว่าผู้ประมวลผลข้อมูลดำเนินงานตามข้อตกลงภายใต้สัญญา อย่างครบถ้วนทุกข้อหากผู้ประมวลผลข้อมูลมีการจ้างช่วงองค์กรอื่นเพื่อให้ความช่วยเหลือในการประมวลผลข้อมูล (ผู้รับจ้างรายย่อย) จะต้องแจ้งสถานศึกษา/องค์กรผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษรเกี่ยวกับการจ้างช่วงนั้น โดยสถานศึกษา/องค์กรผู้ควบคุมข้อมูลจะต้องมีทางเลือกที่จะปฏิเสธหรือแสดงข้อคิดเห็นอันขัดแย้งต่อการจ้างช่วงดังกล่าวได้

ข้อควรหลีกเลี่ยง

ผู้ให้บริการ Third-Party ไม่ควรได้รับอนุญาตให้สามารถเข้าถึงเครือข่าย ไฟล์เอกสาร หรืออาคาร สำนักงานที่เก็บข้อมูลของสถานศึกษา (ผู้ควบคุมข้อมูล) โดยปราศจากการกำกับดูแลอย่างใกล้ชิด แม้เพียงเป็นระยะเวลาสั้นๆ หากยังไม่ได้ทำสัญญาข้อตกลงการประมวลผลข้อมูลระหว่างกันเมื่อเสร็จสิ้นความสัมพันธ์ระหว่างกันตามสัญญา ผู้ให้บริการ Third-Party ไม่ควรได้รับอนุญาต ให้เก็บข้อมูลที่ถูกเปิดเผยโดยองค์กรสถานศึกษาเอาไว้ โดยควรโอนย้ายข้อมูลคืนหรือลบทำลายข้อมูล เว้นเสียแต่มีภาระผูกพันทางกฎหมายหรือความจำเป็นต้องเก็บรักษาต่อภายใต้วัตถุประสงค์การดำเนินงาน บางประการ สถานศึกษาไม่ควรติดต่อผู้ให้บริการ Third-Party เป็นผู้ประมวลผลข้อมูลให้กับองค์กรเพียงเพราะ ได้รับคำแนะนำมา แต่ต้องมีขั้นตอนของการตรวจเช็กและประเมินขีดความสามารถ คุณสมบัติ และ มาตรฐานการดำเนินงานว่าสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง PDPA หรือไม่ ก่อนการทำสัญญาใช้บริการ

กรณีที่ 8: การจัดการด้านความมั่นคงปลอดภัยข้อมูล

ความล้มเหลวในการปกป้องคุ้มครองข้อมูลส่วนบุคคลให้ปลอดภัยเป็นหนึ่งในสาเหตุหลักที่ส่งผลให้เกิดการละเมิด ซึ่งสร้าง ความเสียหายต่อองค์กรกรอย่างมหาศาล เนื่องจากทำลายความเชื่อมั่นของผู้คนที่มีต่อองค์กร กระทบต่อชื่อเสียงและความน่าเชื่อถือของพนักงานและกระบวนการจัดการข้อมูลขององค์กรการจัดสรรความรับผิดชอบบุคลากรระดับสูงของสถานศึกษาควรเป็นผู้รับผิดชอบหลักเกี่ยวกับข้อมูลที่ถูกเก็บรักษาโดยองค์กรกร ควบคุมว่ามีบุคคลใดที่สามารถเข้าถึงได้ เก็บรักษาไว้ที่ใด และถ่ายโอนหรือโอนย้ายไปที่อื่นด้วยวิธีการใด อย่างไร โดยบุคลากร/เจ้าหนาที่ที่สามารถเข้าถึงข้อมูลได้ทุกคนจะต้องนึกคำนึงถึงความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และบริหารจัดการข้อมูลซึ่งเป็นสินทรัพย์อันมีค่ายิ่ง ไม่ว่าจะเป็นข้อมูลที่อยู่ในรูปแบบเอกสารกระดาษหรือ อิเล็กทรอนิกส์ก็ตามการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลของแต่ละองค์กรกรนั้นแต่กต่างกัน ขึ้นอยู่กับจำนวน มูลค่า และรูปแบบของข้อมูลที่เก็บรักษา โดยสถานศึกษาอาจมีมาตรการอย่างเช่น การเข้ารหัสข้อมูล (Encryption) ข้อมูลบนคอมพวเตอร์แล็ปท็อป สมาร์ทโฟน และอุปกรณเก็บข้อมูลต่างๆ การตั้งพาสเวิร์ดเพื่อปกป้อง ไฟล์ทั้งหมดที่เก็บรักษาข้อมูลอ่อนไหว และการใส่กุญแจตู้เก็บเอกสารในสำนักงานเมื่อไม่ได้มีการใชงาน เป็นต้น องค์กรควรพิจารณาแบ่งประเภทของข้อมูลออกจากกันอย่างชัดเจน เพื่อจะได้ปรับใช้มาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมกับชุดข้อมูลที่เกี่ยวข้องกับด้านการแพทย์หรือด้านสภาวะทางจิตใจของนักเรียน หรือบุคลากร กล่าวคือ ข้อมูลจำพวกบันทึกการสัมภาษณ์และการให้คำปรึกษาควรได้รับการคุ้มครองในระดับสูงสุด ควบคู่กับการคุ้มครองข้อมูลส่วนบุคคลทางกายภาพในพื้นที่ของสถานศึกษา ไม่ว่าจะเป็นการจำกัดจำนวนผู้ถือกุญแจเข้าถึงพื้นที่เก็บข้อมูลตลอดจนการติดกล้อง CCTV เพื่อดูแลสอดส่องสถานที่ดังกล่าว

<u>ข้อควรปฏิบัติ</u>

สถานศึกษาควรมีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลที่แสดงให้เห็นถึงระเบียบขององค์กร ในการนำข้อมูลไปใช้ การจัดเก็บ การโอนย้ายและใครบางที่มีสิทธิหรืออำนาจเข้าถึงข้อมูลบุคลากรผู้ที่มีสิทธิ์เข้าถึงข้อมูลทุกคนควรได้รับการฝึกอบรมเกี่ยวกับภาระหนาที่ของต้น ให้คุนเคย กับนโยบายด่านคว่ามปลอดภัย และสามารถประมวลผลข้อมูลภายใต้มาตรฐานที่เหมาะสม หลังสิ้นสุดระยะเวลาของการเปดเผยหรือใชงานข้อมูลส่วนบุคคล (ที่ได้รับคว่ามยินยอมลวงหนา) บุคลากร/เจ้าหนาที่ควรถูกอบรมให้เก็บเอกสารหรือสิงที่มีข้อมูลส่วนบุคคลเหลานั้น กลับสูสำนักงาน บริหารของสถานศึกษา หรือพ้นที่เก็บรักษาข้อมูลขององค์กรกรอย่างรวดเร็วที่สุดหลาย ๆ ครั้ง บุคลากรของสถานศึกษาก็จำเป็นต้องถือครองข้อมูลส่วนบุคคลเอาไว้ที่ตนเอง เพื่อบริหารจัดการนักเรียนภายในห้องเรียนและเพื่อเตรียมการสอน (ลิสต์รายชื่อนักเรียน รายละเอียดการติดต่อผู้ปกครอง) โดยไม่อาจหลีกเลี่ยงได้ อย่างไรก็ตาม บันทึกข้อมูลควรถูกเก็บรักษาไว้เท่าที่จำเป็นและควรถูกรักษาไว้ สถานศึกษาควรสำรองข้อมูล (Backup) เอาไว้ในรูปแบบอิเล็กทรอนิกส์เพื่อที่จะได้สามารถดำเนินการตามปกติได้อย่างทันท่วงทีหากเกิดเหตุภัยพบัติ (อย่างความเสียหายจากไฟไหม้หรือน้ำท่วม) ขึ้นกับสำนักงาน ผู้บริหารระดับสูงควรรับทราบถึงระดับการเข้าถึงข้อมูลนักเรียนและผู้ปกครองของบุคลากร โดยบุคลากรที่สามารถเข้าถึงข้อมูลได้ควรมีหน้าที่เฉพาะเจาะจงที่เกี่ยวของกับชุดข้อมูลนั้น หากองค์กรกรมีการจ้างวานบริษัท Third-Party ในการจัดการข้อมูลควรมีการทำสัญญาข้อตกลง การประมวลผลข้อมูลอย่างเป็นทางการก่อนข้อมูลส่วนบุคคลใดๆ ขององค์กรกรจะถูกเปิดเผยต่อบริษัทนั้น คอมพิวเตอร์ขององค์กรควรได้รับการปกปองด้วยการเข้ารหัสและรหัสทั้งหมดไม่ควรถูกแชร์ระหว่างบุคลากรของสถานศึกษา หรือทิ้งเอาไว้ให้สามารถเข้าถึงได้โดยง่าย องค์กรกรสถานศึกษาควรปรับใชแนวปฏิบัติ 5 ส ในพื้นที่เก็บล็อคแฟ้มเอกสารทุกครั้งหลังการทำงานในแต่ละวันหรือเมื่อไม่ได้ใช้งาน และล็อคประตูเข้า-ออกไม่มีผู้มีอำนาจหนาที่เกี่ยวของกับข้อมูลอยู่ประจำสำนักงาน บุคลากรควรล็อคหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อลุกออกจากโต๊ะทำงาน แม้จะเป็นเพียงระยะเวลาสั้น ๆอย่างปลอดภัยขณะถูกโอนย้ายหรือกำลังถูกใช้งานโดยเฉพาะเวลาเข้าร่วมการประชุมนอกสถานที่ เป็นต้น

เมื่อมีผู้ออกจากงานหรือย้ายองค์กร ความสามารถในการเข้าถึงข้อมูลของบุคคลนั้นควรถูกถอดถอน หรือเปลี่ยนแปลงอย่างเหมาะสมอย่างรวดเร็วที่สุดเท่าที่จะเป็นไปได้ การฝึกอบรมควรถูกจัดขึ้นเป็นประจำอย่างเหมาะสม เพื่อกระตุ้นบุคลากรในทุกระดับของสถานศึกษา เกี่ยวกับด้านการคุ้มครองข้อมูลหากคุณมีการติดตั้งกล้อง CCTV ในพื้นที่ของสถานศึกษา ผู้บริหารระดับสูง (ที่เกี่ยวข้อง) ควรได้รับความไว้วางใจให้เป็นผู้ดูแลด้านการจัดการและการซ่อมบำรุงของระบบและอุปกรณ์อย่างใกล้ชิด

ข้อควรหลีกเลี่ยง

ผู้ที่สามารถเข้าถึงข้อมูลไม่ควรเก็บข้อมูลไว้ในอุปกรณ์ที่ปราศจากการเข้ารหัสและระบบรักษาความปลอดภัย เช่น คอมพิวเตอร์หรือสมาร์ทโฟนส่วนตัวที่ไม่ได้ตั้งรหัสเข้าเครื่องและหากเป็นไปได้ หลีกเลี่ยงการใช้เครือข่ายสาธารณะเพื่อจัดการหรือสื่อสารข้อมูลส่วนบุคคล โดยควรใช้เครือข่ายเฉพาะ/ส่วนตัว ที่มีระบบการเข้ารหัส และมีการรักษาความปลอดภัยสูง เอกสารกระดาษไม่ควรถูกโยกย้ายออกจากสำนักงานขององค์กร/สถานศึกษา นอกเสียจากมีความจำเป็นที่ไม่สามารถหลีกเลี่ยงได้เท่านั้น สำเนาเอกสารข้อมูลเมื่อใช้งานเสร็จควรถูกเก็บรวบรวมกลับสู่สำนักงานอย่างรวดเร็วที่สุด และหากมีสำเนา

กรณีที่ 9: การจัดการเมื่อเกิดการละเมิดและการแจ้งเตือน การจัดสรรความรับผิดชอบ

หากเกิดเหตุละเมิด ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องแจ้งเหตุการละเมิดแกสำนักงานโดยไม่ชักชา (ภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุ) ยกเวนแต่การละเมิดดังกลาวไม่มีคว่ามเสี่ยงที่จะมีผลกระทบต่อสิทธิและ เสรภาพของบุคคล และในกรณีที่การละเมิดมีคว่ามเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรภาพของบุคคลต้อง แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบพรอมกับแนวทางการเยียวยาโดยไม่ชักช้าเช่นกัน (PDPA มาตรา 37)

ข้อควรปฏิบัติ

เมื่อองค์กรกรสถานศึกษาทราบถึงการละเมิด เจ้าหน้าที่คุ้มครองข้อมูลหรือสมาชิกผู้บริหารระดับสูง ควรเป็นผู้ที่ได้รับมอบหมายให้เป็นผู้จัดการดูแลและตรวจสอบเกี่ยวกับเหตุการณ์ดังกล่าวควรให้ผู้ที่เกี่ยวของทุกคนเล่าหรือเพิ่มเติมบันทึกข้อมูลเกี่ยวกับเหตุละเมิด สาเหตุการเกิด ตลอดจนความเสียหายและผลกระทบจากการละเมิดกรณีที่มีเหตุการณใดๆ ที่ส่งผลให้ข้อมูลส่วนบุคคลอาจมีความเสี่ยง (ไม่ว่าจะเป็นการทำรายละเอียดการติดต่อ/รายละเอียดบัญชีสูญหาย การเปดเผยข้อมูลส่วนตัวผ่านการรับคำปรึกษา และอื่น ๆ) สถานศึกษาควรแจ้งผ่านองทางการติดต่อที่เหมาะสมให้เจ้าของข้อมูลส่วนบุคคลทราบถึงความเสี่ยงดังกล่าว และผลกระทบที่อาจเกิดข้นโดยรวดเร็วที่สุดหาก Third-Party ของสถานศึกษา (เช่น บริการทางไอทีหรือหุ้นส่วน) มีความเกี่ยวข้องกับการละเมิดในส่วนใดส่วนหนึ่ง องค์กรเหลานี้จะต้องรายงานเกี่ยวกับเหตุการณที่เกิดขึ้นตลอดจนรีบดำเนิน การแก้ไขอย่างรวดเร็วและเกิดประโยชน์สูงสุด องค์กรกรสถานศึกษาควรแจ้งเหตุละเมิดไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อย่างรวดเร็วที่สุดเมื่อทราบรายละเอียด หรือภายในระยะเวลา 72 ชั่วโมงหลังจากแรกทราบเกี่ยวกับเหตุการณที่เกิดขึ้น (PDPA มาตรา 37) เมื่อพบความผิดปกติของระบบหรือกระบวนการที่อาจกอให้เกิดความไม่มั่นคงปลอดภัยหรือความผิดพลาด สถานศึกษาควรหยุดการใชข้อมูลนั้นในทันทีจนกระทั่งสาเหตุของปัญหาถูกระบุและได้รับการแก้ไข เมื่อทราบถึงสาเหตุของการละเมิด บุคลากร/เจ้าหน้าที่ภายในสถานศึกษาควรได้รับการแจ้งให้ทราบ และได้รับการฝึกอบรมอย่างเหมาะสม เพื่อให้ความเสี่ยงที่เหตุการณ์ละเมิดจะบานปลายลดเหลือน้อยที่สุด กรณีการละเมิดเกิดขึ้นจากความผิดพลาดในการจัดการข้อมูลส่วนบุคคลของบุคลากรหรือนักเรียน ภายในองค์กร สถานศึกษา ควรวางมาตรการลงโทษทางวินัยต่อผู้เกี่ยวข้องอย่างเหมาะสม และสร้างการตระหนักรู้เกี่ยวกับระเบียบนี้เพื่อป้องกันไม่ให้เกิดเหตุการณ์แบบนี้ซ้ำขึ้นอีก การสื่อสารขององค์กรสถานศึกษาที่เกี่ยวของกับเหตุละเมิดข้อมูลควรกำกับดูแลและจัดการโดย เจ้าหนาที่คุมครองข้อมูลหรือผู้บริหารระดับอาวุโส เพื่อลดการสื่อสารที่อาจผิดพลาดและสรางความเชื่อมั่น ลดความเสี่ยงด้านความกังวลใจของผู้ปกครองและนักเรียนที่มีส่วนเกี่ยวข้องสถานศึกษาควรจัดฝึกอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับกระบวนการการตรวจจับ การตรวจสอบ และการแจ้งเตือน เมื่อมีการละเมิดข้อมูลส่วนบุคคลเหลือใช้หรือไม่ได้ใช้งานแล้ว ควรถูกทำลายทิ้งทันทีหลังจากเสร็จสิ้นกิจกรรมหรือวัตถุประสงค์

ข้อควรหลีกเลี่ยง

หลีกเลี่ยงการปกปิดข้อมูลเกี่ยวกับเหตุการณ์ละเมิด หากบุคลากรท่านใดมีคำถามหรือข้อสังสัย ควรติดต่อเจ้าหน้าที่คุ้มครองข้อมูลหรือผู้บริหารระดับอาวุโสที่ได้รับมอบหมายให้เป็นผู้จัดการกับเหตุละเมิดเวลาคือปัจจัยสำคัญ สถานศึกษาไม่ควรปล่อยให้กระบวนการแจ้งเตือนผู้ที่เกี่ยวของล่าช้าต่อทั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและนักเรียนหรือผู้ปกครองในฐานะเจ้าของข้อมูลส่วนบุคคล

กรณีที่ 10: การขอใช้ “สิทธิเข้าถึงข้อมูลส่วนบุคคล” ของเจ้าของข้อมูล

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล (PDPA มาตรา 30) โดยบุคคลใดก็ตามที่ต้องการใช้สิทธิ์ตามข้อกฎหมายดังกล่าวจะต้องส่ง “คำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล” ไปยังผู้ควบคุมข้อมูล แม้ไม่มีแบบฟอร์มอย่างเป็นทางการ แต่คำขอดังกล่าวควรมีลักษณะคือ 1) คำขอควรมีลักษณะเป็นลายลักษณ์อักษร จะเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ และ 2) คำขอต้องมีข้อมูลยืนยันตัวตนของผู้ขอใช้สิทธิอย่างเพียงพอ

ข้อควรปฏิบัติ

องค์กรสถานศึกษาควรดำเนินการยืนยันตัวตนของผู้ขอใชสิทธิอย่างรวดเร็วที่สุดหลังได้รับคำขอ เข้าถึง/รับสำเนาข้อมูลส่วนบุคคล และไม่ควรมีข้อมูลใดที่ถูกค้นหาหรือตรวจสอบก่อนการยืนยันตัวตน เสร็จสิ้น สถานศึกษามีเวลาตอบสนองต่อสูงสุดภายใน 30 วันนับตั้งแต่ได้รับคำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคล อย่างไรก็ตามองค์กร อาจพยายามตอบสนองต่อคำขอภายในระยะเวลาสั้นที่สุดเทาที่ทำได้สถานศึกษาควรมอบหมายบุคลากรให้เป็นผู้ประสานงานในการค้นหารวบรวมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้ขอใช้สิทธิ์ โดยควรเริ่มดำเนินการค้นหาและรวบรวมข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลอย่างชัดเจนอย่างรวดเร็วที่สุด กรณีที่องค์กร Third-Party เป็นผู้จัดเก็บบันทึกข้อมูล บุคลากรที่ได้รับมอบหมายให้ประสานงานของสถานศึกษาควรติดต่อดูแลให้องค์กร Third-Party เหล่านี้ค้นหาเฉพาะข้อมูลที่เกี่ยวข้องและสอดคล้องกับเจ้าของข้อมูลผู้ขอใช้สิทธิ์เข้าถึง/รับสำเนาข้อมูลส่วนบุคคลเอกสารบางตัวที่อาจพาดพิงเกี่ยวข้องกับบุคคลอื่นนอกเหนือจากผู้ขอใช้สิทธิ์เข้าถึง/รับสำเนา ข้อมูลส่วนบุคคล ควรได้รับการแก้ไขให้เหลือเพียงแต่ข้อมูลของผู้ใชสิทธิ์ฯเท่านั้นเมื่อเสร็จสิ้นกระบวนการค้นหาข้อมูลส่วนบุคคล สำเนาของข้อมูลชุดดังกล่าวควรถูกปริ๊นออกมาใน รูปแบบเอกสารกระดาษและจัดส่งไปยังผู้ขอให้สิทธิฯ ผ่านไปรษณีย์แบบลงทะเบียน เพื่อให้มีหลักฐาน ยืนยันการนำส่งเอกสารของสถานศึกษาองค์กร สถานศึกษาองค์กรควรมีสำเนาของเอกสารฉบับเต็มที่ส่งไปยังผู้ขอใช้สิทธิ์เข้าถึง/รับสำเนา ข้อมูลส่วนบุคคล สำรองเอาไว้เผื่อกรณีเกิดขอพิพาทเกี่ยวกับเนื้อหาขอบเขตของเนื้อหาของเอกสารฉบับนี้ตามมาภายหลังสถานศึกษาอาจปฏิเสธคำขอเข้าถึง/รับสำเนาข้อมูลส่วนบุคคลในกรณีที่เป็นการปฏิเสธตามกฎหมาย หรือคำสั่งศาลหรือการเข้าถึงหรือขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อที่ก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น (PDPA มาตรา 30)

ข้อควรหลีกเลี่ยง

องค์กรสถานศึกษาไม่อาจคิดค่าบริการจากการตอบรับคำขอใช้สิทธิ์เข้าถึง/รับสำเนาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ เว้นเสียแต่เป็นคำขอสำเนาของเอกสารเดิมซ้ำๆ (สามารถคิดค่าบริการอย่างสมเหตุสมผล) ข้อมูล/เอกสารต้นฉบับที่เก็บรักษาโดยองค์กรไม่ควรถูกเปิดเผยเป็นส่วนหนึ่งของการตอบสนอง ต่อคำขอใชสิทธิ์เข้าถึง/รับสำเนาข้อมูลส่วนบุคคลสถานศึกษาไม่จำเป็นต้องหาข้อมูลที่อยู่ในระบบ Back-up เนื่องจากไม่มีพันธะตามกฎหมาย ให้จัดทำสำเนาเฉพาะข้อมูลที่กำลังอยู่ในระบบการเก็บรักษาข้อมูลขององค์กรในขณะนั้น

PDPA Thailand

เราคือผู้เชี่ยวชาญดานการคุมครองขอมูลสวนบุคคลภายใต้พระราชบัญญัติคุมครอง ขอมูลสวนบุคคล พ.ศ. 2562 (PDPA) มีบริการหลากหลายที่ตอบโจทยองค์กรทุกกลุม

https://bit.ly/37cwtjm,
www.pdpa.online.th, www.pdpathailand.com

บริการจัดทำและให้คำปรึกษาโดยทีมผู้เชี่ยวชาญกฎหมาย พรอมดูแลองค์กรให้ปฏิบัติตามกฎหมายคุมครองข่อมูลสวนบุคคลได้อยางถูกต่อง

PDPA Compliance Audit สอบทานและตรวจสอบการเตรียมการดานการคุ่มครองข่อมูลสวนบุคคลตามกฎหมาย เพื่อสรางความมั่นใจแกองค์กรที่ทำ PDPA ดวยตนเอง

Outsourced DPO (PDPA)

บริการเปนเจาหนาที่คุมครองขอมูลสวนบุคคล (DPO) ขององค์กรสำหรับองค์กรที่จำเปนตองมี DPO แต่ไม่มีบุคลากรที่มีความพร่อมหรือเตรียมการบุคลากรไม่ทัน

PDPA Document Templates

เทมเพลตเอกสารที่จำเปนตามกฎหมายคุ่มครองข่อมูลสวนบุคคล ปรับใชงายตามบริบทขององค์กร

PDPA Training and Workshop

อบรมและฝกปฏิบัติเพื่อพัฒนาบุคลากรภายในองค์ กร (In-house Training)ดานการคุมครองขอมูลสวนบุคคล เฉพาะคณะทำงานดาน PDPA, DPO, หรือพนักงานทั้งองคกร หรือรวมเรียนในหลักสูตรที่ DBC เปดให้บุคคลทั่วไปเขาอบรม (Public Training)

PDPA E-learning

อบรมการคุมครองขอมูลสวนบุคคลผานระบบออนไลนทุกที่ทุกเวลา โดยวิทยากรชั้นนำของ ประเทศที่เชี่ยวชาญดานการคุมครองขอมูลสวนบุคคล เนื้อหาครอบคลุมทุกดานที่จำเปนตอ การทำให้องค์กรพรอมสำหรับการปฏิบัติตามกฎหมายคุมครองขอมูลสวนบุคคล

PDPA Certification

รวมทดสอบความรู้ ความสามารถทางดานการคุมครองขอมูลสวนบุคคลของบุคลากรในองค์กร เพื่อรับวุฒิบัตรวัดระดับความเขาใจดานการคุมครองขอมูลสวนบุคคลตั้งแต่พื้นฐาน ปฏิบัติการเฉพาะสายงาน หรือขั้นสูงรับรองการเปน DPO โดยวุฒิบัตรจาก DDTI และสถาบันชั้นนำของประเทศและของโลก

PDPA Thailand Starter Kit

รวบรวมบริการตาง ๆ ดานการคุมครองขอมูลสวนบุคคลสำหรับองคกรตั้งแต่เริ่มตนผนวกกับการประกันภัยดานขอมูลสวนบุคคลให้องคกร (PDPA Insurance) เพื่อประกันความเสี่ยงที่อาจเกิดขึ้นแมดำเนินการอยางรอบคอบครอบคลุม