คู่มือ
การดำเนินงานให้สอดคล้อง
กับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
สำหรับภาคีรับทุนโครงการจาก สสส.

เพื่อให้ภาคีผู้รับทุนสนับสนุนโครงการจากกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) ที่มีกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่เกิดจากกิจกรรมภายใต้โครงการให้สามารถดำเนินการให้สอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่ง สสส. ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ตระหนักในการปกป้องคุ้มครองข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมจากโครงการให้ทุนดังกล่าว มิให้ข้อมูลส่วนบุคคลรั่วไหลหรือถูกนำไปใช้ในทางที่มิชอบ หรือนำไปใช้หรือเปิดเผยนอกเหนือจากวัตถุประสงค์ที่ระบุไว้ในโครงการรับทุน และลดความเสี่ยงไม่ให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลที่ภาคีผู้รับทุนโครงการได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

1. การเก็บรวบรวมข้อมูลส่วนบุคคล

หากโครงการมีการเก็บรวบรวมข้อมูลส่วนบุคคล ผ่านการจัดกิจกรรมต่าง ๆ เช่น การจัดประชุมสัมมนา การสัมภาษณ์กลุ่มตัวอย่าง งานวิ่ง การจัดกิจกรรมดูงาน เป็นต้น ตัวอย่างข้อมูลส่วนบุคคลที่จัดเก็บ เช่น ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ ที่อยู่ ภาพถ่าย ภาพเคลื่อนไหว เสียง หรือข้อมูลอื่น ๆ ที่เป็นข้อมูลส่วนบุคคล จะต้องดำเนินการดังต่อไปนี้

1.1 ต้องประกาศความเป็นส่วนตัว (Privacy Notice) ทุกครั้ง

การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องแจ้งวัตถุประสงค์และรายละเอียดต่างๆ ตามที่ PDPA ได้กำหนดไว้ โดยเนื้อหาในประกาศความเป็นส่วนตัว (Privacy Notice) ที่จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ อย่างน้อยจะต้องประกอบด้วย ฐานการประมวลผล (ฐานกฎหมาย) วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลที่จัดเก็บ ระยะเวลาในการจัดเก็บ การส่งข้อมูลไปยังบุคคลหรือหน่วยงานอื่น สิทธิของเจ้าของข้อมูลส่วนบุคคล และข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล *(ควรแยกเขียนเป็นข้อ ๆ ใน Privacy Notice)* สามารถดูตัวอย่างได้จาก QR Code ด้านล่าง หรือตัวอย่างที่ สสส. ได้จัดทำไว้

หมายเหตุ *การประกาศความเป็นส่วนตัว (Privacy Notice) ไม่ต้องให้เจ้าของข้อมูลส่วนบุคคลต้องเซ็นยินยอมหรือลงนามใด ๆ เพราะเป็นการประกาศให้ทราบถึงวัตถุประสงค์ของการจัดเก็บรวบรวม และรายละเอียดตาม PDPA ที่ได้กำหนดไว้*

ตัวอย่าง ประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัว (Privacy Notice)
ของผู้รับทุนและผู้ร่วมโครงการ

ประกาศความเป็นส่วนตัวฉบับนี้จึงจัดทำขึ้นเพื่อให้ท่านในฐานะ ผู้รับทุนและผู้ร่วมโครงการ (ซึ่งต่อไปในประกาศนี้เรียกว่า “เจ้าของข้อมูลส่วนบุคคล”) ได้ทราบและเข้าใจรูปแบบ วิธีการ และวัตถุประสงค์และความจำเป็นของกองทุนสนับสนุนการสร้างเสริมสุขภาพ (“สสส.”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ที่ต้องดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีรายละเอียดดังต่อไปนี้

1. ฐานกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคล

สสส. จำเป็นต้องดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านภายใต้ฐานกฎหมาย โดยมีรายละเอียดดังต่อไปนี้

(1) ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามสัญญา โดยนำข้อมูลส่วนบุคคลของท่านไปใช้ประโยชน์ในการพิจารณาโครงการ ตรวจสอบการมีส่วนได้เสีย (COI) การอนุมัติโครงการ การจัดทำข้อตกลง การเบิกจ่าย

สามารถดูตัวอย่างได้จาก QR Code ด้านล่าง

วิธีการประกาศความเป็นส่วนตัว (Privacy Notice) อาจทำได้หลายวิธี เช่น นำไปแนบต่อท้ายแบบสอบถามหรือ Google form หรือทำเป็น QR code หรือทำเป็น Link ให้คลิกอ่านผ่านระบบ เป็นต้น โดยการประกาศ Privacy Notice สามารถประกาศก่อนหรือระหว่างการเก็บรวบรวมข้อมูลส่วนบุคคล

1.2 การขอความยินยอม (Consent)

การเก็บรวบรวมข้อมูลส่วนบุคคล นอกจากที่จะต้องประกาศความเป็นส่วนตัว (Privacy Notice) แล้ว แต่หากมีการจัดเก็บข้อมูลส่วนบุคคลที่เข้าข่าย ดังต่อไปนี้ 1) การจัดเก็บข้อมูลอ่อนไหว (personal sensitive data) ตามมาตรา 26 (ไม่รวมที่กฎหมายยกเว้น) 2) จัดเก็บข้อมูลสำหรับใช้ในการโฆษณาประชาสัมพันธ์ หรือ 3) การจัดเก็บข้อมูลส่วนบุคคลที่ไม่สามารถเลือกใช้ฐานการประมวลผลใด ๆ ได้ ตามมาตรา 24 หรือมาตรา 26 (ไม่รวมที่กฎหมายยกเว้น) เมื่อเข้าข่ายข้อใดข้อหนึ่งดังกล่าวจะต้องขอความยินยอมโดยใช้ฐานความยินยอม (Consent) โดยเจ้าของข้อมูลส่วนบุคคลสามารถเลือก “ยินยอม” หรือ “ไม่ยินยอม” ได้ และสามารถถอนความยินยอมเมื่อไหร่ก็ได้ *(หากไม่เข้าข่าย 3 ข้อข้างต้น ไม่ต้องทำข้อ 1.2 นี้)*

โดยทั่วไปการขอความยินยอมมักจะให้เจ้าของข้อมูลส่วนบุคคลคลิกเลือก “ยินยอม” หรือ “ไม่ยินยอม” ของเรื่องนั้น ๆ ที่ขอความยินยอม

ข้อมูลอ่อนไหวตามมาตรา 26 ได้แก่ การจัดเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ รวมถึงข้อมูลอ่อนไหวอื่น ๆ ตามประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่ได้ประกาศเพิ่มเติม (ถ้ามี)

ตัวอย่าง การเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลสุขภาพ โดยใช้ฐานความยินยอม (Consent)

กรณี การแพ้อาหาร

โปรดระบุชื่ออาหาร/ประเภทอาหาร ที่ท่านแพ้.....

วัตถุประสงค์ของการจัดเก็บชื่ออาหาร/ประเภทอาหาร ที่แพ้ เพื่อจะได้จัดอาหาร/ประเภทอาหาร ให้ท่านได้อย่างถูกต้องและปลอดภัยต่อสุขภาพของท่าน

☐ ยินยอม ให้จัดเก็บอาหาร/ประเภทอาหาร ที่แพ้

☐ ไม่ยินยอม ให้จัดเก็บอาหาร/ประเภทอาหาร ที่แพ้

<u>หมายเหตุ</u> กรณีที่ท่านแพ้อาหาร แต่ไม่ยินยอมให้จัดเก็บอาหาร/ประเภทอาหาร ที่แพ้ ท่านอาจไม่ได้รับความสะดวกในการจัดอาหารให้ท่านได้อย่างถูกต้องในการเข้าร่วมงานครั้งนี้

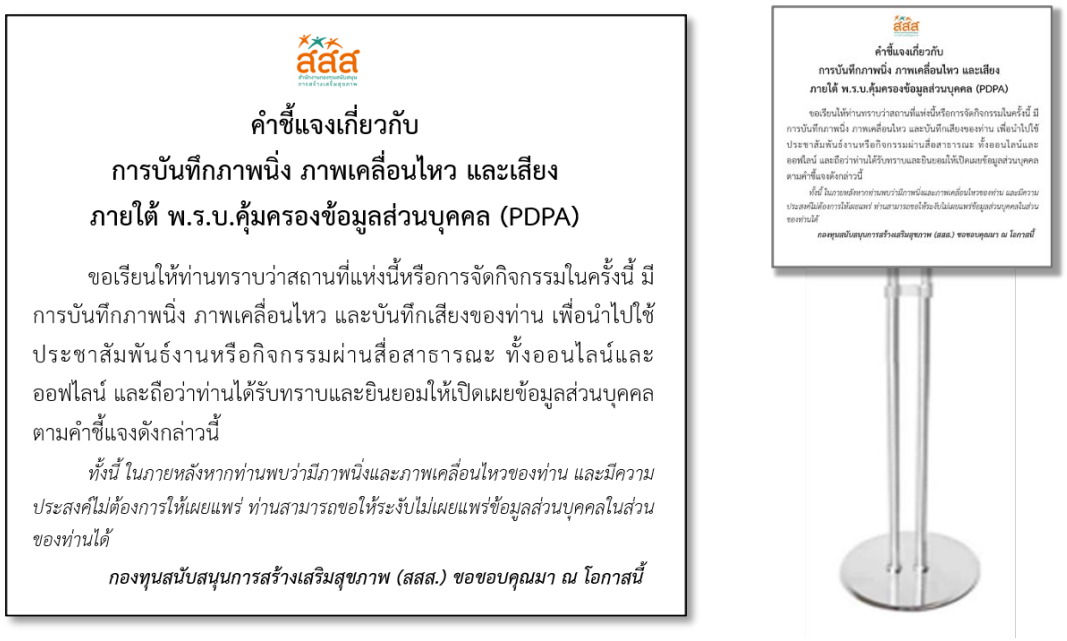
กรณีหากมีใช้สำเนาบัตรประจำตัวประชาชนเพื่อใช้เป็นหลักฐานประกอบการเบิกจ่ายหรือการทำธุรกรรม 1) ควรให้เจ้าของข้อมูลส่วนบุคคลหรือภาคี ทำการขีดฆ่าหรือป้ายสีทับข้อมูล "ศาสนา" เพราะศาสนาถือเป็นข้อมูลอ่อนไหวตามมาตรา 26 แต่หากโครงการใช้ข้อมูลศาสนาสำหรับประกอบการจัดทำโครงการจะต้องให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม 2) ให้เจ้าของข้อมูลส่วนบุคคล ขีดคร่อม เซ็นกำกับ บนสำเนาบัตรประชาชน เพื่อป้องกันหากข้อมูลรั่วไหล

1.3 การติดป้ายประกาศกลางแจ้ง

กรณีที่โครงการมีการจัดเก็บข้อมูลส่วนบุคคลของผู้ร่วมกิจกรรม ในลักษณะที่มีผู้ร่วมงานเป็นจำนวนมาก หรืออาจมีบุคคลที่ไม่ได้ลงทะเบียนเข้าร่วมงานที่ไม่ได้ทราบประกาศความเป็นส่วนตัว (Privacy Notice) หรือไม่ได้ขอความยินยอมมาก่อน และในงานได้มีการจัดเก็บภาพถ่าย ภาพเคลื่อนไหว และการบันทึกเสียงของผู้เข้าร่วมงาน ดังนั้นจึงจำเป็นต้องจัดทำประกาศเพื่อขอความยินยอมอีกครั้ง เช่น งานวิ่งที่มีผู้เข้าร่วมจำนวนมาก งานจัดอีเวนต์ งานประชุมสัมมนา ที่มีผู้ร่วมงานทั้งได้รับเชิญหรือไม่ได้รับเชิญ หรืองานถ่ายทำภาพยนตร์/คลิป ที่อาจมีบุคคลอื่น ๆ ผ่านเข้ามาในฉากการถ่ายทำโดยไม่ได้ตั้งใจ เป็นต้น

การติดป้ายประกาศกลางแจ้ง ให้ทำเป็นป้ายปิดประกาศไว้บริเวณในงานหรือหน้างาน เช่น ถ้าเป็นงานประชุมสัมมนา อาจทำเป็นป้ายตั้งไว้หน้าห้องประชุมสัมมนา *(หมายเหตุ การปิดป้ายประกาศกลางแจ้งไม่ได้เป็นการบังคับว่าทุกกิจกรรมจะต้องดำเนินการ ขึ้นกับความเหมาะสมตามเหตุผลข้างต้น)*

ตัวอย่างการติดป้ายประกาศกลางแจ้ง



คำชี้แจงเกี่ยวกับ
การบันทึกภาพนิ่ง ภาพเคลื่อนไหว และเสียง
ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

ขอเรียนให้ท่านทราบว่าสถานที่แห่งนี้หรือการจัดกิจกรรมในครั้งนี้ มีการบันทึกภาพนิ่ง ภาพเคลื่อนไหว และบันทึกเสียงของท่าน เพื่อนำไปใช้ประชาสัมพันธ์งานหรือกิจกรรมผ่านสื่อสาธารณะ ทั้งออนไลน์และออฟไลน์ และถือว่าท่านได้รับทราบและยินยอมให้เปิดเผยข้อมูลส่วนบุคคลตามคำชี้แจงดังกล่าวนี้

ทั้งนี้ ในภายหลังหากท่านพบว่ามีภาพนิ่งและภาพเคลื่อนไหวของท่าน และมีความประสงค์ไม่ต้องการให้เผยแพร่ ท่านสามารถขอให้ระงับไม่เผยแพร่ข้อมูลส่วนบุคคลในส่วนของท่านได้

กองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) ขอขอบคุณมา ณ โอกาสนี้

หมายเหตุ ตามตัวอย่างประกาศข้างต้น ด้านล่างของประกาศให้เปลี่ยนเป็นชื่อของภาคี (หน่วยงาน/องค์กร) ได้

1.4 การจัดเก็บข้อมูลส่วนบุคคลของผู้เยาว์ หรือคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

หากโครงการมีการเก็บรวบรวมข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ หรือคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ ต้องดำเนินการดังนี้ 1) หากเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์มีอายุไม่เกินสิบปี ให้ผู้ใช้อำนาจปกครองให้ความยินยอมแทน 2) หากเจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ ให้ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถให้ความยินยอมแทน 3) หากเจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ ให้ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถให้ความยินยอมแทน

กรณีผู้เยาว์อายุมากกว่า 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์ ผู้เยาว์สามารถให้ความยินยอมได้ด้วยตนเองตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์

1.5 การเก็บรวบรวมข้อมูลส่วนบุคคลมาจากแหล่งอื่น

กรณีที่ภาคีผู้รับทุนได้ดำเนินกิจกรรมภายใต้โครงการ ไม่ได้จัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง แต่ได้มีการจัดเก็บข้อมูลหรือได้ข้อมูลมาจากแหล่งอื่น เช่น มีการขอข้อมูลหรือส่งข้อมูลส่วนบุคคลมาจากหน่วยงานอื่น เพื่อนำมาใช้ในกิจกรรม/โครงการ หรือเพื่อใช้ประกอบการวางแผนบริหารจัดการโครงการ เป็นต้น หากยังไม่ได้มีการขอความยินยอมหรือเจ้าของข้อมูลส่วนบุคคลยังไม่รับทราบ ภาคีผู้รับทุนจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 30 วันนับตั้งแต่วันที่เก็บรวบรวม และต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นกรณีที่ได้รับการยกเว้นตามกฎหมายที่ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2. การใช้หรือการเปิดเผย ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่เกิดจากการดำเนินกิจกรรมภายใต้โครงการ จะต้องใช้หรือเปิดเผยภายในขอบเขตดังต่อไปนี้

1) ใช้หรือเปิดเผยตามวัตถุประสงค์ที่กำหนดไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือแจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล
2) ใช้หรือเปิดเผยตามที่เจ้าของข้อมูลได้ให้ความยินยอมไว้ (เว้นแต่ได้รับการยกเว้นตามมาตรา 24 หรือ 26)
3) การเปิดเผยหรือส่งข้อมูลส่วนบุคคล ไปยังบุคคลหรือหน่วยงานอื่นต้องแจ้งหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน (เว้นแต่ได้รับการยกเว้นตามมาตรา 24 หรือ 26)
4) หากมีวัตถุประสงค์การใช้ใหม่ ที่แตกต่างจากวัตถุประสงค์เดิมที่ได้แจ้งไว้ จะต้องแจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอีกครั้ง

<u>หมายเหตุ</u> กรณีที่ภาคีรับทุนโครงการทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ของโครงการนั้นๆ ตามที่ สสส. ได้กำหนดให้นั้น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกิดจากกิจกรรมภายใต้โครงการ ต้องเป็นไปตามสัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) กับ สสส.

3. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ภาคีผู้รับทุนโครงการ จะต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เกิดจากการดำเนินกิจกรรมภายใต้โครงการ ประกอบไปด้วยการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย

1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็นตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น
3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว รวมถึงการลงทะเบียนและการถอนสิทธิ การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน การทบทวนสิทธิการเข้าถึง การถอดถอนหรือปรับปรุงสิทธิการเข้าถึงของผู้ใช้งาน
4) การกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล
6) กรณีที่ต้องส่งข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ไปให้แก่บุคคลหรือนิติบุคคลอื่น ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

4. การลบหรือทำลายข้อมูลส่วนบุคคล

กรณีที่ภาคีผู้รับทุนโครงการ ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของโครงการนั้น ๆ จะต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวตามมาตรา 37(3) และถือว่าเป็นส่วนหนึ่งของความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เช่น ป้องกันการรั่วไหลของข้อมูล ดังนั้นจะต้องลบหรือทำลายข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้

1) เมื่อพ้นกำหนดระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นตามที่ระบุไว้ในประกาศความเป็นส่วนตัว (Privacy Notice)
2) เมื่อข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น
3) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือทำลายข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
4) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการจัดเก็บ ใช้ หรือเปิดเผย ตามที่กฎหมายกำหนด

<u>หมายเหตุ</u> สามารถยกเว้นไม่ต้องลบหรือทำลายข้อมูลส่วนบุคคลได้ ให้เป็นไปตามที่ PDPA ได้กำหนดไว้ หรืออาจทำข้อมูลส่วนบุคคลดังกล่าวให้เป็นข้อมูลนิรนาม (anonymous data)

ส่วนกรณีที่ภาคีผู้รับทุนโครงการ ทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ของโครงการนั้น ๆ การลบหรือทำลายข้อมูลส่วนบุคคลของโครงการ จะต้องดำเนินการภายใต้ขอบเขตที่ได้ตกลงไว้กับ สสส. หรือรายละเอียดตามที่ได้กำหนดไว้ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

5. การลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

มาตรา 40 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ข้อตกลงดังกล่าวเรียกอีกอย่างหนึ่งว่า “ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)”

สสส. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ที่ได้สนับสนุนทุนโครงการให้แก่ภาคี ซึ่งบทบาทของภาคีผู้รับทุนจะแบ่งเป็นสองลักษณะตาม PDPA ดังนี้ 1) ภาคีผู้รับทุนโครงการเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของโครงการนั้น ๆ หรือ 2) ภาคีผู้รับทุนโครงการเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ของโครงการนั้น ๆ

ภาคีผู้รับทุนโครงการที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล*ตามคำสั่งหรือในนามของ สสส.*

โดยสำนัก/ฝ่าย ของ สสส. ที่ให้ทุนโครงการจะเป็นผู้กำหนดให้เองว่าโครงการนั้น ๆ ภาคีผู้รับทุนทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล

(Data Processor) ดังนั้นหากโครงการไหนภาคีผู้รับทุนทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) **จะต้อง**ลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับ สสส.

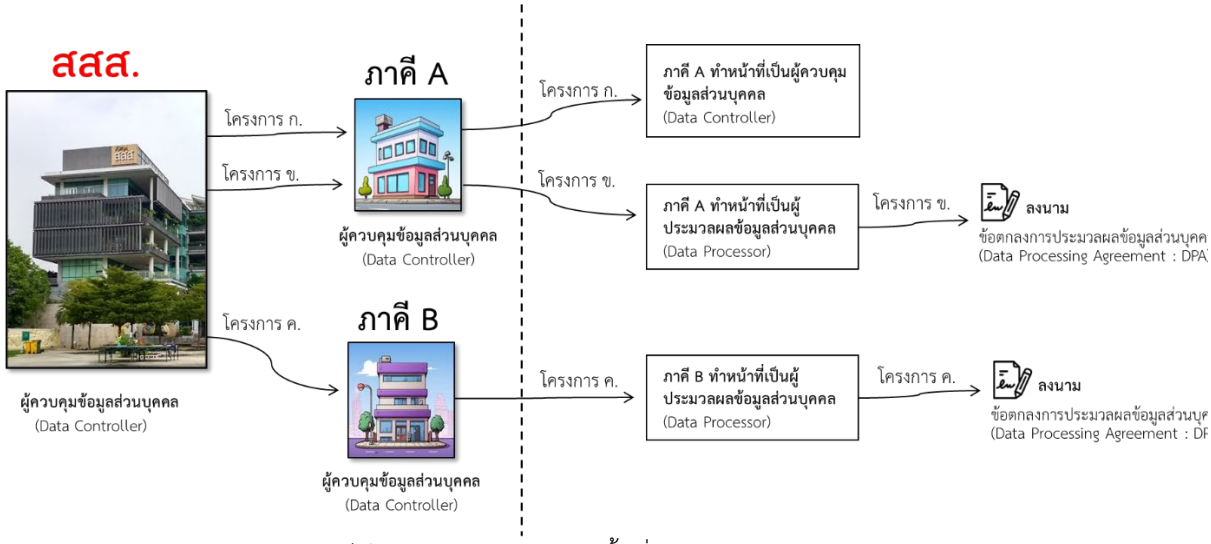
แต่หากภาคีรับทุนทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของโครงการนั้น ๆ **ไม่ต้อง**ลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับ สสส.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ถือว่าเป็นส่วนหนึ่งของสัญญา ซึ่งภาคีผู้รับทุนต้องดำเนินการตามรายละเอียดของข้อตกลงดังกล่าวอย่างเคร่งครัด

ตาราง แสดงตัวอย่างของโครงการ ที่ภาคีผู้รับทุนทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และภาคีผู้รับทุนทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

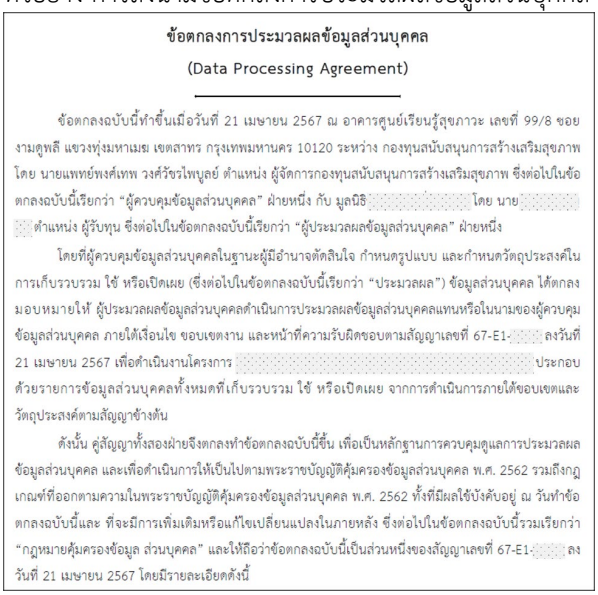
โครงการที่ภาคีทำหน้าที่เป็น ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	โครงการที่ภาคีผู้รับทุนทำหน้าที่เป็น ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)
1. จัดซื้อจัดจ้างทำของที่ระลึก (เสื้อ, ถุงผ้า, ปฏิทิน) 2. ใช้บริการพัสดุไปรษณีย์ 3. จ้างซ่อมบำรุงนิทรรศการสืบสร้างสุข 4. จัดทำชุดข้อมูลและพัฒนาสื่อเผยแพร่องค์ความรู้สุขภาวะ 5. จัดจ้างผลิตภาพยนตร์โฆษณาฯ 6. โครงการทุนอุปถัมภ์ 7. จ้างทีมตรวจภายนอก (IA) หรืองานที่เป็นวิชาชีพอิสระ 8. สำนัก/ฝ่าย จ้างภาคีดำเนินโครงการ (โดยภาคีเป็นผู้วางแผนการ ดำเนินการและวิธีการเก็บรวบรวม ใช้ และเปิดเผย เอง) เช่น การรับทุนประเภทแผนงาน (program) หรือประเภทชุดโครงการ (project package) หรือโครงการประเภทร่วมทุน	1. จ้างภาคีไปจัดเก็บข้อมูล (Survey, Poll) ที่มีข้อมูลส่วนบุคคล (แบบสอบถาม, ผ่านระบบ) 2. นำข้อมูลส่วนบุคคลที่สำนัก/ฝ่ายดูแลอยู่ไปจ้างภาคีภายนอกวิเคราะห์ (Data Analytics) 3. การนำข้อมูลไปฝากไว้บนคลาวด์ของบริษัทภายนอก 4. จ้างบริษัทรับดูแลเว็บไซต์ระบบสมาชิกของ สสส. (สำนัก/ฝ่าย) 5. จ้างบริษัทพัฒนาระบบ (มีข้อมูลส่วนบุคคล) 6. จ้างบริษัทจัดทำเงินเดือน สำหรับเจ้าหน้าที่ ลูกจ้าง 7. ใช้บริการระบบบัญชีจากผู้ให้บริการภายนอก (ฐานข้อมูลอยู่ที่ผู้ให้บริการภายนอก) 8. สำนัก/ฝ่าย จ้างภาคีดำเนินโครงการ (โดยสำนัก/ฝ่ายเป็นผู้วางแผนการดำเนินการ และวิธีการเก็บรวบรวม ใช้ และเปิดเผย เอง)
ไม่ต้องลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) กับ สสส.	ต้องลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) กับ สสส.

แสดงตัวอย่างโครงการที่จะต้องลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)



จากแผนภาพข้างต้นจะเห็นได้ว่ามีบางโครงการเท่านั้นที่จะต้องลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) โดยสำนัก/ฝ่าย จะเป็นผู้กำหนดเองว่าโครงการไหนต้องลงนาม DPA หรือไม่ (เลือกในระบบบริหารโครงการ) หากเป็นทำสัญญาแบบอิเล็กทรอนิกส์ระบบบริหารโครงการจะทำ DPA ผ่านระบบให้เลย (พร้อมกับสัญญาหลักของโครงการรับทุน)

ตัวอย่าง การลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)



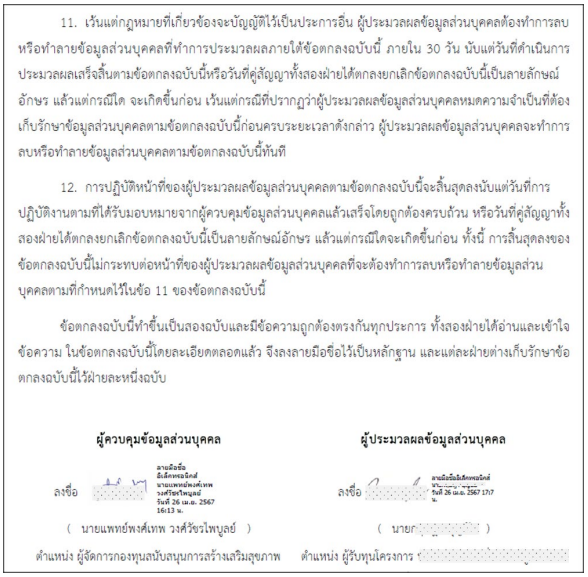
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

(Data Processing Agreement)

ข้อตกลงฉบับนี้ทำขึ้นเมื่อวันที่ 21 เมษายน 2567 ณ อาคารศูนย์เรียนรู้สุขภาวะ เลขที่ 99/8 ซอยงามดูพลี แขวงทุ่งมหาเมฆ เขตสาทร กรุงเทพมหานคร 10120 ระหว่าง กองทุนสนับสนุนการสร้างเสริมสุขภาพ โดย นายแพทย์พงศ์เทพ วงศ์วัชรไพบูลย์ ตำแหน่ง ผู้จัดการกองทุนสนับสนุนการสร้างเสริมสุขภาพ ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า "ผู้ควบคุมข้อมูลส่วนบุคคล" ฝ่ายหนึ่ง กับ มูลนิธิ[redacted] โดย นาย[redacted] ตำแหน่ง ผู้รับทุน ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า "ผู้ประมวลผลข้อมูลส่วนบุคคล" ฝ่ายหนึ่ง

โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลในฐานะผู้มีอำนาจตัดสินใจ กำหนดรูปแบบ และกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย (ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า "ประมวลผล") ข้อมูลส่วนบุคคล ได้ตกลงมอบหมายให้ ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ภายใต้เงื่อนไข ขอบเขตงาน และหน้าที่ความรับผิดชอบตามสัญญาเลขที่ 67-E1-[redacted] ลงวันที่ 21 เมษายน 2567 เพื่อดำเนินงานโครงการ [redacted] ประกอบด้วยรายการข้อมูลส่วนบุคคลทั้งหมดที่เก็บรวบรวม ใช้ หรือเปิดเผย จากการดำเนินการภายใต้ขอบเขตและวัตถุประสงค์ตามสัญญาข้างต้น

ดังนั้น คู่สัญญาทั้งสองฝ่ายจึงตกลงทำข้อตกลงฉบับนี้ขึ้น เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคล และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎเกณฑ์ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และ ที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง ซึ่งต่อไปในข้อตกลงฉบับนี้รวมเรียกว่า "กฎหมายคุ้มครองข้อมูล ส่วนบุคคล" และให้ถือว่าข้อตกลงฉบับนี้เป็นส่วนหนึ่งของสัญญาเลขที่ 67-E1-[redacted] ลงวันที่ 21 เมษายน 2567 โดยมีรายละเอียดดังนี้



11. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลภายใต้ข้อตกลงฉบับนี้ ภายใน 30 วัน นับแต่วันที่ดำเนินการประมวลผลเสร็จสิ้นตามข้อตกลงฉบับนี้หรือวันที่คู่สัญญาทั้งสองฝ่ายได้ตกลงยกเลิกข้อตกลงฉบับนี้เป็นลายลักษณ์อักษร แล้วแต่กรณีใด จะเกิดขึ้นก่อน เว้นแต่กรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลหมดความจำเป็นที่ต้องเก็บรักษาข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ก่อนครบระยะเวลาดังกล่าว ผู้ประมวลผลข้อมูลส่วนบุคคลจะทำการลบหรือทำลายข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ทันที

12. การปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลแล้วเสร็จโดยถูกต้องครบถ้วน หรือวันที่คู่สัญญาทั้งสองฝ่ายได้ตกลงยกเลิกข้อตกลงฉบับนี้เป็นลายลักษณ์อักษร แล้วแต่กรณีใดจะเกิดขึ้นก่อน ทั้งนี้ การสิ้นสุดลงของข้อตกลงฉบับนี้ไม่กระทบต่อหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลที่จะต้องทำการลบหรือทำลายข้อมูลส่วนบุคคลตามที่กำหนดไว้ในข้อ 11 ของข้อตกลงฉบับนี้

ข้อตกลงฉบับนี้ทำขึ้นเป็นสองฉบับและมีข้อความถูกต้องตรงกันทุกประการ ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความ ในข้อตกลงฉบับนี้โดยละเอียดตลอดแล้ว จึงลงลายมือชื่อไว้เป็นหลักฐาน และแต่ละฝ่ายต่างเก็บรักษาข้อตกลงฉบับนี้ไว้ฝ่ายละหนึ่งฉบับ

ผู้ควบคุมข้อมูลส่วนบุคคล

ลงชื่อ [redacted]

(นายแพทย์พงศ์เทพ วงศ์วัชรไพบูลย์)

ตำแหน่ง ผู้จัดการกองทุนสนับสนุนการสร้างเสริมสุขภาพ

ผู้ประมวลผลข้อมูลส่วนบุคคล

ลงชื่อ [redacted]

(นาย[redacted])

ตำแหน่ง ผู้รับทุนโครงการ [redacted]

6. การดำเนินการกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

หากโครงการรับทุนพบเหตุการละเมิดหรือข้อมูลส่วนบุคคลรั่วไหล ที่เกิดจากการดำเนินกิจกรรมของโครงการ เช่น แบบสอบถามที่มีข้อมูลส่วนบุคคลสูญหาย คอมพิวเตอร์โน๊ตบุ๊คที่มีข้อมูลส่วนบุคคลเกิดการสูญหาย ข้อมูลสุขภาพรั่วไหล ถูกเจาะระบบ เป็นต้น

6.1 กรณีภาคีรับทุนทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของโครงการนั้น ๆ ให้ดำเนินการดังต่อไปนี้

1) ประเมินความเสี่ยงของเหตุการละเมิดที่เกิดขึ้น หากเหตุการละเมิดนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ภาคีผู้รับทุนแจ้งเหตุการละเมิดนั้นแก่**สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล** ภายในกำหนดเวลาไม่เกิน 72 ชั่วโมง นับแต่เวลาที่ทราบเหตุการละเมิดนั้น แต่หากพิจารณาแล้วพบว่าเหตุการดังกล่าวไม่ก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของบุคคล ไม่ต้องแจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2) กรณีที่พิจารณาแล้วเห็นว่า เหตุการละเมิดนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ภาคีรับทุนโครงการแจ้งเหตุการละเมิดนั้นพร้อมกับแนวทางการจัดการเหตุการละเมิดนั้น ให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

3) ให้บันทึกข้อมูลเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นทุกกรณี เพื่อจัดเก็บไว้เป็นหลักฐานการตรวจสอบและการบริหารจัดการ

6.2 กรณีภาคีรับทุนทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ของโครงการนั้น ๆ ให้ดำเนินการดังต่อไปนี้

1) ประเมินความเสี่ยงของเหตุการละเมิดที่เกิดขึ้น หากเหตุการละเมิดนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ภาคีผู้รับทุนแจ้งเหตุการละเมิดนั้นแก่**กองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.)** ภายในกำหนดเวลาไม่เกิน 72 ชั่วโมง นับแต่เวลาที่ทราบเหตุการละเมิดนั้น แต่หากพิจารณาแล้วพบว่าเหตุการละเมิดดังกล่าวไม่ก่อให้เกิดความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของบุคคล ไม่ต้องแจ้งมายัง สสส.

2) ส่วนที่จะแจ้งมายัง สสส. ประกอบด้วยหัวข้อดังต่อไปนี้ รายละเอียดของเหตุละเมิดข้อมูลส่วนบุคคล วันเวลาที่ทราบเหตุ ประเภทข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ผลกระทบหรือความเสียหายที่อาจเกิดขึ้น มาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล และรายละเอียดการติดต่อภาคีผู้รับทุนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของภาคี (ถ้ามี)

สามารถดาวน์โหลดเอกสารเพิ่มเติมตาม QR code นี้