เวอร์ชันกำกับ: Guideline การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็น
Version 1.0
วันที่ออกเอกสาร วันที่ 10 มกราคม 2565

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็น

แม้ว่าเราจะเก็บและใช้ข้อมูลส่วนบุคคลอย่างตรงไปตรงมาและตามที่กฎหมายกำหนด แต่เราไม่สามารถเก็บข้อมูลส่วนบุคคลนานกว่าที่เราจำเป็นต้องใช้ นอกจากนี้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุให้กำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็น โดยพิจารณาตามจุดประสงค์ที่เราระบุไว้ การจัดเก็บข้อมูลตามระยะเวลาเท่าที่จำเป็นจะช่วยลดความเสี่ยงที่ข้อมูลจะไม่สอดคล้องตามขอบเขตและวัตถุประสงค์ที่กำหนด รวมทั้งเก็บเกินความจำเป็น (ตามหลักเกณฑ์ Purpose Limitation) หรือข้อมูลไม่ถูกต้อง หรือข้อมูลที่จัดเก็บล้าสมัย (ตามหลักเกณฑ์ Accuracy)

เราควรทำอย่างไรกับข้อมูลส่วนบุคคลที่มีระยะเวลาเกินกว่าที่จำเป็นต้องใช้

หลังจากที่ครบกำหนดตามตามที่ระบุระยะเวลาไว้ใน**นโยบายความเป็นส่วนตัว (Privacy Notice)** เราจำเป็นต้องมีการลบหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้หลังจากที่ข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นต้องใช้ การไม่ดำเนินการดังกล่าวอาจทำให้ผู้ควบคุมข้อมูล ในที่นี้คือมหาวิทยาลัยมหิดล ไม่สามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ ในทางปฏิบัติ การจัดเก็บข้อมูลเกินกว่าระยะเวลาที่จำเป็นจะทำให้ต้องมีค่าใช้จ่ายที่ไม่จำเป็นที่เกี่ยวข้องกับการจัดเก็บและรักษาความปลอดภัยของข้อมูล ดังนั้นจะต้องดำเนินการตามที่ได้แจ้งไว้

แนวทางในการกำหนดระยะเวลาเท่าที่จำเป็น

1. ทำไมคุณจำเป็นต้องทำ

การวางแผนลบหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ ต้องทำทั้งที่เป็นสารสนเทศประเภทกระดาษและดิจิตอล ทั้งการจัดเก็บสารสนเทศที่อยู่ในรูปแบบดิจิตอลต่างๆ เช่น

- สารสนเทศที่ดำเนินการในระบบอิเล็กทรอนิกส์ที่หลากหลายทั้งในและนอกหน่วยงาน
- ระบบจัดการข้อมูลและสารสนเทศอิเล็กทรอนิกส์ต่างๆ
- ไดรฟ์ที่จัดเก็บส่วนบุคคลและใช้ร่วมกัน เช่น Google Drive หรือ My Site หรือ One Drive
- ฐานข้อมูลต่างๆ
- อีเมลล์ และ ที่เก็บสำรองอีเมลล์
- Social Media เช่น facebook twitter Line ของหน่วยงาน

โอกาส

นอกจากความจำเป็นที่ต้องทำตามกฎหมายแล้ว การลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ จะช่วยเพิ่มโอกาสให้หน่วยงานเกี่ยวกับ

- **ลดค่าใช้จ่ายในการจัดเก็บและบำรุงรักษา** โดยการแยกสารสนเทศที่จำเป็นในการดำเนินการออก
- **เพิ่มประสิทธิภาพ** โดยทำให้สารสนเทศที่จำเป็นสามารถค้นหาและใช้ได้ง่ายขึ้น
- **สนับสนุนการปฏิบัติตามกฎหมาย**

ความเสี่ยง

การจัดเก็บสารสนเทศนานกว่าที่หน่วยงานต้องการจะเพิ่มความเสี่ยงดังต่อไปนี้

- **ค่าใช้จ่าย** หน่วยงานจำเป็นต้องเสียค่าใช้จ่ายจำนวนมากในการบำรุงรักษาและจัดทำที่เก็บสำรองเพื่อให้สามารถนำสารสนเทศดิจิตอลกลับมาใช้งานได้ ยิ่งมีสารสนเทศมากเท่าใด คุณจำเป็นต้องมีค่าใช้จ่ายในการจัดเก็บมากขึ้น ซึ่งอาจรวมถึงโอกาสที่ค่าปรับจากข้อมูลรั่วไหลอีกด้วย
- **ประสิทธิภาพ** การจัดเก็บสารสนเทศมากเกินไปจะหน่วงประสิทธิภาพของระบบสารสนเทศ และทำให้ยากต่อการค้นหาสารสนเทศ และทำให้การดำเนินการธุรกรรมต่างๆ ไม่มีประสิทธิภาพเท่าที่ควร

- **ชื่อเสียง** การที่หน่วยงานไม่ลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ จะส่งผลต่อความเสี่ยงในการไม่ปฏิบัติตามกฎหมาย และมีโอกาสถูกฟ้องร้องได้

2. สารสนเทศอะไรที่คุณจำเป็นต้องมี

ในการพิจารณาว่าสารสนเทศอะไรที่เราจำเป็นต้องมี อาจต้องพิจารณาประเด็นดังต่อไปนี้

เรามีสารสนเทศอะไรบ้าง

ก่อนอื่นเราจำเป็นต้องศึกษาเกี่ยวกับหน่วยงานว่าเราทำอะไร และเข้าใจกระบวนการดำเนินงานของเราให้ชัดเจน อาทิ กระบวนการที่เราต้องรับผิดชอบ โดยอาจใช้วิธีการสำรวจในการค้นหาสารสนเทศที่จำเป็นต้องมี สำหรับวิธีการสำรวจมีหลายวิธีขึ้นกับความพร้อมและความเหมาะสมของแต่ละหน่วยงาน เช่น

- สำรวจภาพรวมทั้งหน่วยงาน โดยอาจใช้กลุ่ม facilitators ช่วยในการดำเนินการผลักดันให้เกิดการวิเคราะห์ขึ้น ข้อดีของวิธีนี้คือดึงการมีส่วนร่วม ทำให้เห็นภาพใหญ่ได้ และสามารถเห็นความเชื่อมโยงได้ แต่ต้องใช้ทรัพยากรจำนวนมาก อาจไม่สามารถลงรายละเอียดได้ชัด และในหน่วยงานขนาดใหญ่อาจทำได้ยาก
- สำรวจตามกลุ่มพันธกิจหรือการดำเนินการ โดยอาจใช้กลุ่ม facilitators ช่วยในการดำเนินการผลักดันให้เกิดการวิเคราะห์ขึ้นเช่นกัน ข้อดีคือทำให้เข้าใจในระบบงานได้ดี แต่ต้องใช้ระยะเวลานานขึ้นในการดำเนินการให้ครบทุกกลุ่ม
- ให้ผู้รับผิดชอบแต่ละพันธกิจสำรวจตามสารสนเทศที่ใช้ในการดำเนินการ โดยอาจใช้ตัวแทนผู้รับผิดชอบในการให้ข้อมูล เนื่องจากผู้รับผิดชอบในแต่ละพันธกิจจะเข้าใจในกระบวนการดำเนินการได้ดีอยู่แล้ว แต่ข้อเสียคือกลุ่มผู้รับผิดชอบจะไม่ค่อยว่างและอาจไม่ให้ความสำคัญจากการดำเนินการ

หลังจากนั้นให้ทำการระบุสารสนเทศอะไรที่ต้องเก็บรวบรวม ใช้ เปิดเผย และทำลาย ทั้งนี้เราจะต้องพิจารณาประเภทของสารสนเทศทั้งหมดไม่ว่าจะรูปแบบใด ทั้งรูปแบบกระดาษหรืออิเล็กทรอนิกส์

เราจัดเก็บสารสนเทศที่ไหน

ขั้นตอนต่อไปคือ ค้นหาว่าเราเก็บสารสนเทศที่เราต้องดำเนินการที่ใดบ้าง ทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ ในกรณีที่สารสนเทศอยู่ในระบบอิเล็กทรอนิกส์ จะต้องพิจารณาหรือวางแผนจัดเก็บในรูปแบบใด

นอกจากนี้อาจต้องเข้าใจเกี่ยวกับวงจรชีวิตของเทคโนโลยี เช่นคาดการณ์อายุการใช้งานของระบบ หรือจะต้องย้ายสารสนเทศเมื่อใด และความเชื่อมโยงระหว่างระบบ โดยส่วนนี้เจ้าหน้าที่ระบบสารสนเทศอาจช่วยสนับสนุนได้ ซึ่งจะทำให้การตัดสินใจในการเลือกระบบการใช้งานได้ดีขึ้น

การสำเนาสารสนเทศ

นอกจากรู้สถานที่จัดเก็บแล้ว จำเป็นต้องรู้เกี่ยวกับการทำสำเนาสารสนเทศดังกล่าวด้วย เพื่อที่จะทำการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้

ทำการบันทึกสิ่งที่คุณรู้

ควรที่จะบันทึกสารสนเทศที่คุณจำเป็นต้องใช้ลงในฐานข้อมูลหรือ Excel โดยแนะนำให้อยู่ในบันทึกรายการกิจกรรมการประมวลผล (ROPA) โดยอย่างน้อยที่สุดควรมีข้อมูลดังต่อไปนี้

- ประเภทสารสนเทศข้อมูลส่วนบุคคล
- ผู้รับผิดชอบสารสนเทศหลัก
- ระยะเวลาในการจัดเก็บ แนวทางการทำลาย
- เหตุผลของการจัดเก็บ และใช้ฐานกฎหมายอะไร
- มีข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่
- การเข้าถึงข้อมูลส่วนบุคคล
- ข้อมูลส่วนบุคคลมีการจัดเก็บที่ไหน

โดยบันทึกรายการกิจกรรมการประมวลผล (ROPA) จะต้องทำการรวบรวมทั้งหมด ยืนยันลงนามโดยหัวหน้าส่วนงานหรือผู้ที่หัวหน้าส่วนงานมอบหมาย และนำส่งผ่านระบบ Mysite ให้กับ DPO ของมหาวิทยาลัยมหิดล เพื่อทำการรวบรวมและใช้ประเมินในกรณีที่มีเหตุการณ์ละเมิด ตามที่กฎหมายกำหนด

ทำการทบทวนให้เป็นปัจจุบัน

การทำการบันทึกรายการกิจกรรมการประมวลผล (ROPA) ไม่ใช่การดำเนินการครั้งเดียว เนื่องจากหน่วยงานมีการเปลี่ยนแปลง และผู้รับผิดชอบมีการเปลี่ยนแปลง ดังนั้นการบันทึกรายการกิจกรรมการประมวลผล (ROPA) จำเป็นต้องมีการทบทวนตามระยะเวลาที่กำหนด ซึ่งทางหน่วยงานอาจพิจารณาว่าควรมีการทบทวนบ่อยแค่ไหน เช่น ทุกปีหรือในกรณีที่มีการเปลี่ยนแปลง

3. เข้าใจในคุณค่าของสารสนเทศที่คุณจัดเก็บ

ทุกการกระทำที่เกี่ยวกับการจัดการสารสนเทศควรที่จะทำบนฐานที่เข้าใจในคุณค่าของสารสนเทศที่ให้กับหน่วยงาน

ประเภทของคุณค่า

ตัวอย่างประเภทของคุณค่าสารสนเทศมีดังต่อไปนี้

- **สารสนเทศที่จำเป็นต้องเก็บตามกฎหมาย**

  กฎหมายบางประเภทได้มีการกำหนดสารสนเทศใดที่ต้องมีการจัดเก็บ และระยะเวลาการจัดเก็บ เช่น พรบ. ความผิดทางคอมพิวเตอร์ ซึ่งแต่ละพันธกิจภายในหน่วยงานควรทราบเกี่ยวกับสารสนเทศดังกล่าว

- **สารสนเทศที่มีคุณค่าต่อการดำเนินการตามพันธกิจ**

  สารสนเทศนี้จำเป็นเพื่อให้พันธกิจสามารถดำเนินการต่อได้ หรือเป็นหลักฐานต่อการดำเนินการตามพันธกิจ ทั้งนี้จำเป็นต้องทำงานร่วมกับผู้รับผิดชอบแต่ละพันธกิจเพื่อกำหนดสารสนเทศใดที่ต้องจัดเก็บตามจุดประสงค์ที่กำหนด ที่ต้องใช้ในการดำเนินงาน และจำเป็นต้องมีระยะเวลาการจัดเก็บนานเท่าใด

- **สารสนเทศที่มีคุณค่าจากการใช้ซ้ำ**

  ทั้งนี้จำเป็นต้องพิจารณาว่าสารสนเทศใดบ้าง ที่จำเป็นต้องถูกนำมาใช้ซ้ำ หรือนำมาใช้ในการปรับปรุงกระบวนการทำงาน ซึ่งอาจรวมถึงภาครัฐกำหนดให้มีการจัดส่งข้อมูลและสารสนเทศตามที่ได้กำหนดไว้

- **สารสมเทศที่ให้คุณค่าเชิงประวัติศาสตร์**

  สารสนเทศประเภทนี้เพื่อสะท้อนให้เห็นถึงการดำเนินการหรือการตัดสินใจที่สำคัญ เช่น เรื่องอะไร ทำไมต้องทำหรือไม่ทำ และดำเนินการอย่างไร เช่น เอกสารเชิงนโยบายที่สำคัญ บันทึกการตัดสินใจที่สำคัญ เหตุการณ์ที่สำคัญ

การใช้คุณค่าในการตัดสินใจ

เมื่อเข้าใจเกี่ยวกับคุณค่าของสารสนเทศแล้ว จึงค่อยเริ่มตัดสินใจดำเนินการว่าจะจัดการสารสนเทศอย่างไร

- ถ้าสารสนเทศที่คุณดำเนินการมีคุณค่าในระยะสั้น ดังนั้นการจัดเก็บไม่ควรเกินกว่าระยะเวลาการใช้ประโยชน์สารสนเทศดังกล่าว การจัดเก็บระยะนานกว่าการนำไปใช้ประโยชน์ จำเป็นต้องเสียค่าใช้จ่ายในการบำรุงรักษาการสำรอง และต้องให้การเข้าถึงข้อมูลในช่วงเวลาต่างๆ
- ถ้าสารสนเทศที่จัดเก็บมีคุณค่าในระยะปานกลางหรือระยะยาว จะต้องหาหลักฐานหรือเหตุผลประกอบว่าไปสนับสนุนการดำเนินการตามพันธกิจอย่างไร หรือเป็นสารสนเทศที่มีคุณค่าเชิงประวัติศาสตร์ ในกรณีที่คุณยืนยันคุณค่าดังกล่าว จะต้องหากระบวนการหรือระบบที่จะค้นหา การเปิด ป้องกันการรั่วไหล และใช้งานกับสารสนเทศดังกล่าวนานเท่าที่คุณจำเป็นต้องใช้

ต้องมั่นใจว่าบุคลากรเข้าใจในคุณค่าของสารสนเทศดังกล่าว

ต้องมั่นใจว่าบุคลากรที่เกี่ยวข้องทั้งหน่วยงานเข้าใจสารสนเทศอะไรที่จัดเก็บ เก็บที่ไหน และเหตุผลในการจัดเก็บ ตัวอย่างวิธีการได้แก่

- ทำให้เป็นส่วนหนึ่งของการอบรมเบื้องต้นสำหรับบุคลากรใหม่ และเสริมการอบรมเพิ่มเติมเพื่อมั่นใจว่าบุคลากรยังคงมีความรู้เกี่ยวกับเรื่องนี้
- จัดทำเอกสารทั้งในรูปแบบออนไลน์หรือกระดาษ เช่น Infographic หรือ Poster เพื่อแนะนำเกี่ยวกับประเด็นดังกล่าว
- ใช้ผู้แทนสารสนเทศในแต่ละพันธกิจส่งเสริมหรือถ่ายทอดประเด็น เนื้อหาต่างๆ และสนับสนุนให้บุคลากรทำสิ่งที่ถูกต้องตามที่กฎหมายคุ้มครองส่วนบุคคลกำหนด

4. การลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้ เมื่อหมดความต้องการ

มีหลายวิธีการ ทีทำให้เกิดการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้

ตัดสินใจระยะเวลาสิ้นสุดการจัดเก็บ

การตัดสินใจว่าจะลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้จำเป็นต้องมีการกำหนดระยะเวลาการสิ้นสุดการจัดเก็บ ตัวอย่างเช่น

ใช้เวลา ..... ปี หรือตามรอบการทำลายเอกสารในช่วงปีดังกล่าว หลังจากที่ได้รับอนุมัติให้ดำเนินการ.... ดังกล่าว เว้นแต่ต้องใช้เป็นหลักฐานในการดำเนินคดีตามที่ได้รับการร้องขอและจะลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนหลังจากที่ได้รับอนุมัติหรือหมดความจำเป็นดังกล่าว

สร้างกระบวนการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตน กับสารสนเทศประเภทดิจิตอล

ในกรณีที่เป็นไปได้ให้ทำกระบวนการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตน โดยอัตโนมัติในระบบดิจิตอลที่คุณใช้งาน ทั้งนี้ขึ้นกับแต่ละระบบ ระบบที่แตกต่างกันอาจใช้วิธีการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนแตกต่างกัน ส่วนใหญ่จะมีการวางแผน Metadata ในระบบสารสนเทศที่ต้องถูกดำเนินการ ในกรณีที่ไม่สามารถดำเนินการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้โดยอัตโนมัติจะต้องวางแผนช่วงเวลาที่เหมาะสมในการดำเนินการ

สร้างกระบวนการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตน กับสารสนเทศประเภทกระดาษ

ควรมีการกำหนดช่วงระยะเวลาในการทำลายเอกสารที่เป็นกระดาษที่ชัดเจน ประเภทของเอกสารที่ต้องทำลาย และมีการดำเนินการตามรอบระยะเวลาที่กำหนด ซึ่งอาจรวมถึงการแต่งตั้งคณะกรรมการในการดำเนินการดังกล่าว

มีกระบวนการทวนสอบ

ควรมีกระบวนการทวนสอบสารสนเทศใดที่ได้ทำการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้ และดำเนินการเมื่อใด ในกรณีที่ไม่ได้ทำลายโดยอัตโนมัติ ควรมีการกำหนดช่วงระยะเวลาในการทำลายเอกสารให้ชัดเจน

ระบุคำจำกัดความการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตนได้การให้ชัดเจน

การลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตน ในทางดิจิตอลอาจมีความหมายแตกต่างกันได้ ซึ่งการดำเนินการลบ ทำลาย หรือทำให้สารสนเทศไม่สามารถระบุตัวตน ในบางกรณีอาจสามารถฟื้นคืนข้อมูลดิจิตอลให้สามารถกลับมาได้ ดังนั้นจะต้องมีการระบุแนวทางหรือนโยบายให้ชัดเจนเพื่อลดปัญหาดังกล่าว