ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
เรื่อง แนวทางการลบและทำลายข้อมูลส่วนบุคคล

โดยที่มาตรา 37 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม อีกทั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้มีประกาศ เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 เพื่อให้เกิดความชัดเจนในการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา 31 (3) แห่งพระราชกฤษฎีกาจัดตั้งสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. 2548 และที่แก้ไขเพิ่มเติม จึงออกประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง แนวทางการลบและทำลายข้อมูลส่วนบุคคลของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง แนวทางการลบและทำลายข้อมูลส่วนบุคคล”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 แนวทางในการลบและทำลายข้อมูลส่วนบุคคล ให้เป็นตามเอกสารแนบท้ายประกาศนี้

ข้อ 4 ให้ผู้อำนวยการเป็นผู้รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ หรือคำสั่งต่าง ๆ เพื่อปฏิบัติให้เป็นไปตามประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 1 กันยายน พ.ศ. 2568

(นายวิรัตน์ ปราบทุกข์)
ผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง

แนวทางการลบและทำลายข้อมูลส่วนบุคคล
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

****

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา 23 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม ประกอบกับมาตรา ๓๗ (๓) ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จึงได้จัดทำ “แนวทางการลบและทำลายข้อมูลส่วนบุคคล” ขึ้น เพื่อใช้ในแนวทางในการลบและทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม และเพื่อให้เกิดความชัดเจนในการดำเนินงานตามภารกิจของสถาบัน

บทนิยาม

“สถาบัน” หมายความว่า สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

“ผู้ให้บริการภายนอก” หมายความว่า บุคคลหรือนิติบุคคลที่มีนิติสัมพันธ์ตามสัญญากับสถาบันและมีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของสถาบัน

“หน่วยงานความร่วมมือ เครือข่าย สมาคม กลุ่มบุคคล หรือผู้ทำงานร่วมกับสถาบัน” หมายความว่า บุคคลหรือผู้แทนหน่วยงานที่มีความร่วมมือกับสถาบัน ทั้งในรูปแบบการทำงานตามข้อตกลงความร่วมมือ และแนวทางตามนโยบายหรือกระบวนการทำงานในรูปแบบใดรูปแบบหนึ่ง

“การลบและทำลาย” หมายความว่า การทำให้ข้อมูลส่วนบุคคลไม่สามารถบ่งชี้กลับมายังตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้อีก โดยอาศัยวิธีการลบและทำลายต่าง ๆ ที่เหมาะสมตามชนิดหรือรูปแบบของการจัดเก็บข้อมูล

ข้อ 1 การกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

ตามมาตรา 23 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ในการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีการกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลไว้ จึงทำให้สถาบันต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละประเภท ดังนี้

ที่	ประเภทของข้อมูล	สื่อที่ใช้เก็บข้อมูล	ระยะเวลาในการเก็บรักษาข้อมูล
1	ข้อมูลส่วนบุคคลของเกษตรกรบนพื้นที่สูงที่สถาบันให้การส่งเสริมและสนับสนุน ทั้งทางด้านเศรษฐกิจ สังคม สิ่งแวดล้อม และด้านโครงการพื้นฐาน	- Shared Drive ของสถาบัน - ตู้เก็บเอกสาร	ตลอดระยะเวลาการเป็นเกษตรกรที่อยู่ภายใต้การส่งเสริมและสนับสนุนของสถาบัน

ที่	ประเภทของข้อมูล	สื่อที่ใช้เก็บข้อมูล	ระยะเวลาในการเก็บรักษาข้อมูล
2	ข้อมูลส่วนบุคคลของผู้สมัครงาน	- Shared Drive ของสถาบัน - ตู้เก็บเอกสาร	สำหรับผู้สมัครงานที่ไม่ได้รับการแต่งตั้งเป็นผู้ปฏิบัติงาน เก็บรักษาไว้ไม่เกิน 1 ปี นับแต่วันที่สถาบันได้รับข้อมูลส่วนบุคคล
3	ข้อมูลส่วนบุคคลของผู้ปฏิบัติงาน	- Shared Drive ของสถาบัน - ตู้เก็บเอกสาร	สำหรับผู้ปฏิบัติงาน เก็บรักษาไว้ตลอดระยะเวลาการจ้างงาน และเก็บรักษาไว้ต่อไปเป็นเวลา 10 ปี นับแต่วันที่สัญญาจ้างสิ้นสุดลง
4	ข้อมูลส่วนบุคคลของคณะกรรมการ กรรมการผู้ทรงคุณวุฒิ คณะกรรมการตรวจสอบ และคณะอนุกรรมการ	- Shared Drive ของสถาบัน - แฟ้มเอกสารของฝ่ายเลขานุการ	8 ปี นับจากได้รับการแต่งตั้ง หรือเมื่อหมดวาระการดำรงตำแหน่ง (แล้วแต่ระยะเวลาใดจะถึงก่อน)
5	ข้อมูลส่วนบุคคลของเจ้าหน้าที่สถาบัน สำหรับนำมาเป็นฐานข้อมูลประกอบการคำนวณการหักภาษีเงินได้ ณ ที่จ่าย ของสถาบัน	- Shared Drive ของสถาบัน	1 ปี
6	ข้อมูลส่วนบุคคลของนักวิจัย เจ้าหน้าที่สถาบัน เจ้าหน้าที่โครงการหลวง เกษตรกรร่วมวิจัย นักวิจัยท้องถิ่น (ฐานข้อมูลนักวิจัย)	- Shared Drive ของสถาบัน	10 ปี
7	ข้อมูลส่วนบุคคลของเกษตรกร เพื่อวางแผนการดำเนินงานวิจัยที่สอดคล้องกับเป้าหมายของงานวิจัยในแต่ละมิติ และข้อมูลส่วนบุคคลของผู้ที่นำผลงานวิจัยไปใช้ประโยชน์	- Shared Drive ของสถาบัน - ห้องเก็บเอกสาร	10 ปี
8	ข้อมูลส่วนบุคคลของเกษตรกรเพื่อการจัดทำฐานข้อมูลขอบเขตการใช้ประโยชน์ที่ดินรายแปลง และการจัดทำแผนที่ดินรายแปลงของเกษตรกร	- เก็บบน Storage ของ สวพส. และมีการ log-in ตามสิทธิความจำเป็น - server ของ สวพส.	10 ปี
9	ข้อมูลส่วนบุคคลของผู้เข้าร่วมประชุม อบรม สัมมนา	- Shared Drive ของสถาบัน - ห้องเก็บเอกสาร	10 ปี หรือจนกว่าจะสิ้นสุดกระบวนการตรวจสอบตามกฎหมายของสำนักงานการตรวจเงินแผ่นดิน และกระทรวงการคลัง หรือมีการถอนความยินยอม หรือจนกว่าจะสิ้นสุดกระบวนการพิจารณาคดี
10	ข้อมูลส่วนบุคคลจากกล้องวงจรปิด	ระบบ CCTV	ไม่เกิน 30 วัน
11	ข้อมูล Log ทางอิเล็กทรอนิกส์	- เครื่องให้บริการของระบบต่างๆ - ระบบจัดเก็บข้อมูล Log	90 วัน หรือกรณีตามข้อ 12 (2) แห่ง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564
12	ระบบ WIFI Controller	ระบบ WIFI Controller	90 วัน
13	ข้อมูลบัญชีผู้ใช้งานระบบอิเล็กทรอนิกส์ต่างๆ ของสถาบัน	- ระบบพิสูจน์และยืนยันตัวตน - เครื่องให้บริการของระบบต่างๆ	เมื่อสิ้นสุดสัญญาการเป็นเจ้าหน้าที่ของสถาบัน

ข้อ 2 หลักการทำข้อมูลนิรนาม (Anonymization)

แนวทางในการทำลายข้อมูลส่วนบุคคลแบ่งออกเป็น 2 วิธี ดังนี้

2.1 ทำลายสื่อที่ใช้เก็บบันทึกข้อมูลส่วนบุคคล

2.2 การจัดทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization)

การจัดทำข้อมูลนิรนาม คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (Negligible risk) โดยวิธีที่ได้รับความนิยมในการทำข้อมูลนิรนามมีดังนี้

(1) Scrambling การผสมข้อมูล เป็นการสลับลำดับของตัวอักษรในข้อมูลด้วยกฎเกณฑ์หนึ่งๆ อาทิ กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุกช่องข้อมูล ยกตัวอย่างเช่น 012345 กลายเป็น 210345 เป็นต้น

(2) Masking การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูล เช่น ข้อมูลหมายเลขโทรศัพท์ 0987654321 แสดงเป็น ######4321

(3) Blurring or Noising การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนั้นทวีความนิยมมากขึ้นในภาครัฐภาคเอกชนทั่วโลก เช่น มีชุดข้อมูลเป็นสีรถและทะเบียนรถ อาจจะลดข้อมูลเหลือสีรถ

(4) Pseudonymization การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่างๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมา

(5) De-identification การขจัดตัวตน คือการลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่เป็นการป้องกันการย้อนรอยเพื่อระบุตัวตน (re-identification) โดยพิจารณาถึงตัวข้อมูลเป็นหลัก ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย เช่น มีชุดข้อมูล ชื่อ นายจอห์น อีเมล์ john@example.com เบอร์โทร 0987654321 แสดงเป็น นาย A อีเมล - เบอร์โทร -

ข้อ 3 แนวทางการลบและทำลายข้อมูลส่วนบุคคล

3.1 ขั้นตอนการลบและทำลายข้อมูลส่วนบุคคล

3.1.1 หลักเกณฑ์ในการเริ่มต้นกระบวนการ

(1) เมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(2) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้มีการลบหรือทำลาย

3.1.2 ขั้นตอนการปฏิบัติงาน

(1) คณะทำงานปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคล ขออนุญาตลบหรือทำลายข้อมูลส่วนบุคคลที่ครบกำหนดระยะเวลาการเก็บรักษา หรือเจ้าของข้อมูลส่วนบุคคลมีการร้องขอเป็นลายลักษณ์อักษรให้มีการลบหรือทำลาย พร้อมทั้งระบุเหตุผลและวิธีการที่จะใช้ในการลบหรือทำลาย

(2) ผู้อำนวยการสถาบันพิจารณาให้ความเห็นชอบในการลบหรือทำลาย

- กรณีเห็นชอบ ให้ดำเนินการต่อในข้อ (1.3)
- กรณีไม่เห็นชอบ ให้สิ้นสุดกระบวนการ

(3) คณะทำงานปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคลแจ้งผู้รับผิดชอบข้อมูลส่วนบุคคลนั้นเพื่อดำเนินการลบหรือทำลาย ตามแนวทางการลบและทำลายข้อมูลส่วนบุคคลในข้อ 3.2

(4) คณะทำงานปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคลบันทึกหลักฐานการลบหรือทำลาย

(5) คณะทำงานปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคลแจ้งผลการลบหรือทำลายแก่ผู้อำนวยการสถาบัน

3.2 แนวทางการลบและทำลายข้อมูลส่วนบุคคล

ที่	ประเภทสื่อที่จัดเก็บข้อมูล	การลบหรือทำลาย	การทำข้อมูลนิรนาม (Anonymization)
1	บนกระดาษ	• ทำลายด้วยเครื่องทำลายเอกสาร ที่ไม่สามารถนำซากเอกสารที่ทำลาย แล้วมาประกอบและอ่านข้อมูลได้ หรือตามกฎหมายว่าด้วยงานสารบรรณกำหนด	- Masking
2	ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ต่างๆ	• ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่สถาบันกำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ • ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมลส่วนบุคคลได้	Pseudonymization
3	บนเครื่องให้บริการ หรือฐานข้อมูลของระบบสารสนเทศต่างๆ	• ใช้คำสั่งการลบทำลาย (delete) ข้อมูลของระบบบริหารจัดการฐานข้อมูล • ใช้คำสั่งการลบทำลาย (delete) ข้อมูลเครื่องให้บริการระบบ (Virtual Machine) ที่ควบคุมการเข้าถึงข้อมูลนั้น	
4	บนสื่อบันทึกข้อมูลประเภทฮาร์ดดิสก์	• ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่สถาบันกำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ • ใช้การทำลายทางกายภาพ อาทิ - Hard disk ประเภทจานหมุน ทำให้แผ่นเก็บข้อมูลภายในเป็นรอยขีดข่วนร้ายแรง (ทุบ เจาะ บดขยี้) หรือใช้เครื่องทำลายแบบ Degaussing - Hard disk ประเภท SSD ถอดแยกชิ้นส่วนและทำลายแผงวงจรภายในจนไม่สามารถประกอบใช้งานได้ (ทุบ เจาะ บดขยี้) หรือใช้เครื่องทำลายแบบ Degaussing	- Masking - Scrambling - Blurring or noising - Pseudonymization - De-identification เช่น การลบข้อมูล หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์
5	บนสื่อบันทึกข้อมูลประเภทเคลื่อนที่ได้	• ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่สถาบันกำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ อาทิ - ใช้เครื่องทำลาย CD/ DVD หรือหักทำลายเป็นส่วนๆ อย่างน้อย 4 ส่วน - Thumb drive ถอดแยกชิ้นส่วน และทำลายแผงวงจรภายในจนไม่สามารถประกอบใช้งานได้ หรือ De-identification	- Masking - Scrambling - Blurring or noising - Pseudonymization - De-identification เช่น การลบข้อมูล หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์

ที่	ประเภทสื่อที่จัดเก็บข้อมูล	การลบหรือทำลาย	การทำข้อมูลนิรนาม (Anonymization)
		• ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้	
6	บนคลาวด์	• ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่สถาบันกำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ • ใช้คำสั่งการลบทำลาย (delete) เครื่องให้บริการระบบ (Virtual Machine) ที่ควบคุมการเข้าถึงข้อมูลนั้น (ในกรณีที่เป็นการใช้บริการคลาวด์ที่อนุญาตให้มีการสร้างเครื่องให้บริการได้ และไม่มีการใช้งานเครื่องให้บริการนั้นอีกต่อไป) • ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้	

3.3 การจ้างผู้ให้บริการภายนอกให้ดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ในกรณีที่สถาบันว่าจ้างผู้ให้บริการภายนอกให้ดำเนินการลบ ทำลาย หรือดำเนินการใด ๆ เพื่อให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ สถาบันต้องกำกับดูแลและควบคุมกระบวนการดังกล่าวตลอดระยะเวลาดำเนินการ และต้องจัดให้มีการจัดเก็บหลักฐานที่แสดงถึงการทำลายข้อมูลจากผู้ให้บริการภายนอกอย่างครบถ้วนและตรวจสอบได้

3.4 การแจ้งให้หน่วยงานความร่วมมือ เครือข่าย สมาคม กลุ่มบุคคล หรือผู้ทำงานร่วมกับสถาบันดำเนินการลบ ทำลาย หรือดำเนินการใด ๆ เพื่อให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ในกรณีที่สถาบันได้ดำเนินการลบ ทำลาย หรือดำเนินการใด ๆ เพื่อให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ สถาบันต้องแจ้งให้หน่วยงานความร่วมมือ เครือข่าย สมาคม กลุ่มบุคคล หรือผู้ทำงานร่วมกับสถาบันทราบ เพื่อทำการลบ ทำลาย หรือดำเนินการใด ๆ เพื่อให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้นั้นทันที

ข้อ 4 การทบทวนแนวทาง

สถาบันจะดำเนินการทบทวนแนวทางการลบและทำลายข้อมูลส่วนบุคคลนี้อย่างน้อยปีละ 1 ครั้ง
