แนวทางในการลบและทำลายข้อมูลส่วนบุคคล

GUIDELINES FOR PERSONAL DATA DESTRUCTION

โครงการจัดจ้างวิเคราะห์และจัดทำแนวทางมาตรการในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคล ตามโครงการธรรมาภิบาลข้อมูลภาครัฐ กปส. (PRD Data Governance)

JUL 2022

PREPARED BY

THAMMASAT UNIVERSITY
RESEARCH AND CONSULTANCY INSTITUTE
สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

Document Control

Document Owner	กรมประชาสัมพันธ์
Document Preparer	สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์
Date Created	6/15/2022
Date Last Modified	7/22/2022
Document Name	แนวทางในการลบและทำลายข้อมูลส่วนบุคคล Guidelines for personal data Destruction
Version	1.0
Status	Final

Document Change Record

Version	Date Last Modified	By	Details of modification
1.0	7/22/2022	TU	Final

Document Review

Name	Position

Document Approver

Name	Position	Signature	Date
			Click or tap to enter a date.

Contents

Document Control 2

Document Change Record 2

Document Review 2

Document Approver 2

คำนิยาม 1

หลักการและเหตุผล 2

วัตถุประสงค์ 2

ขอบเขต 2

การกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล 3

หลักการทำข้อมูลนิรนาม (Anonymization) 4

แนวทางการลบทำลายข้อมูลส่วนบุคคล 5

1. ขั้นตอนการลบทำลายข้อมูลส่วนบุคคล 5
2. แนวทางการลบทำลายข้อมูลส่วนบุคคล 5
3. การจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล 6

คำนิยาม

คำศัพท์	ความหมาย
องค์กร	กรมประชาสัมพันธ์ (“กปส.”)
ที่ปรึกษา	สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล ชื่อเล่น ที่อยู่ หมายเลขโทรศัพท์ เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) ทะเบียนรถยนต์ IP Address, Cookies, Log File เป็นต้น
การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data)	การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล (อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในลักษณะใดลักษณะหนึ่งได้) เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบ จัดโครงสร้าง การปรับปรุงหรือการแก้ไขข้อมูล การดึงข้อมูล การให้คำปรึกษาที่ต้องใช้ข้อมูลในการให้คำปรึกษา การใช้ข้อมูล การเปิดเผยด้วยการส่งต่อ การเผยแพร่ หรือ การกระทำใด ๆ เพื่อให้ข้อมูลสามารถเข้าถึงหรือใช้งานได้ การรวมข้อมูลเข้าด้วยกัน การดำเนินการเพื่อให้ข้อมูลสอดคล้องกัน การจำกัดการใช้งาน การลบ หรือการทำลายข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่สามารถระบุตัวตนได้จากข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ รวมตลอดทั้งผู้ที่ถือว่าเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	บุคคลหรือองค์กรใดที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลส่วนบุคคล
การจัดทำขอมูลนิรนาม (Anonymization)	กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องใหความสำคัญกับความเสี่ยง (Negligible Risk)

หลักการและเหตุผล

ปัจจุบันเมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศใช้งาน กรมประชาสัมพันธ์ (กปส.) เล็งเห็นถึงความสำคัญของข้อมูลส่วนบุคคลที่กรมฯ จัดเก็บ รวมรวม และมีการใช้งาน ซึ่งจะต้องปฏิบัติให้สอดคล้องกับกฎหมายดังกล่าว ในการดูแลรักษาความมั่นคงปลอดภัยและดำเนินการต่าง ๆ ให้สอดคล้องกับข้อกำหนดของกฎหมาย กปส. จึงจำเป็นต้องจัดจ้างที่ปรึกษาดำเนินการศึกษาและวิเคราะห์เกี่ยวกับ การจัดเก็บ รวบรวม เปิดเผย และใช้งานข้อมูลส่วนบุคคลที่กรมฯ นำมาประมวลผล เพื่อประเมินช่องว่างสถานภาพที่เป็นอยู่เทียบกับข้อกำหนด ความต้องการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และความมั่นคงปลอดภัยของระบบสารสนเทศที่จัดเก็บข้อมูลส่วนบุคคล รวมทั้งการจัดทำ ปรับปรุง นโยบายและแนวปฏิบัติหรือหลักเกณฑ์ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องตามที่กฎหมายกำหนด และสร้างความเชื่อมั่นต่อเจ้าของข้อมูลส่วนบุคคลที่กรมฯ มีการนำข้อมูลส่วนบุคคลมาประมวลผล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 วรรค 3 ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม และมาตรา 37 วรรค 3 ระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา จึงทำให้มีความจำเป็นในการกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล และแนวทางขั้นตอนการลบทำลายข้อมูลส่วนบุคคล

วัตถุประสงค์

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อใช้ในการกำหนดขั้นตอนกระบวนการปฏิบัติการเก็บรักษาข้อมูลส่วนบุคคลและกระบวนการทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดการเก็บรักษาและไม่มีการนำข้อมูลกลับมาประมวลผล หรือเมื่อเจ้าของข้อมูลมีการร้องขอให้ทำลายข้อมูล

ขอบเขต

เอกสารฉบับนี้ประกอบไปด้วยแนวทางการเก็บรักษาข้อมูลส่วนบุคคลและแนวทางการลบทำลายข้อมูลส่วนบุคคล โดยเอกสารฉบับนี้จะถูกนำไปใช้เมื่อมีสถานการณ์การจัดเก็บรักษาข้อมูลส่วนบุคคล และลบทำลายข้อมูลเมื่อสิ้นสุดระยะเวลาการเก็บรักษา

แนวทางการเก็บรักษาข้อมูส่วนบุคคลประกอบไปด้วยระยะเวลาในการเก็บรักษาข้อมูล และสื่อที่ใช้เก็บข้อมูลโดยแยกตามประเภทของข้อมูล

แนวทางการลบทำลายข้อมูลส่วนบุคคลประกอบไปด้วย ขั้นตอนการปฏิบัติการทำลายข้อมูล และแนวทางในการลบทำลายข้อมูล

การกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 วรรค 3 ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม จึงทำให้ต้องกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ประเภทของข้อมูล	สื่อที่ใช้เก็บข้อมูล	ระยะเวลาในการเก็บรักษาข้อมูล
ข้อมูลเจ้าหน้าที่ และผู้บริหาร	เครื่องคอมพิวเตอร์ (PC)	10 ปีหลังสิ้นสุดสภาพการเป็นเจ้าหน้าที่
	กระดาษ	
	ระบบ File Server	
	ระบบสแกนลายนิ้วมือ	
	ระบบ AD	1 สัปดาห์ หลังได้รับการแจ้งวันพ้นสภาพการเป็นเจ้าหน้าที่
ข้อมูลผู้สมัครงาน	กระดาษ	10 ปี นับจากวันที่ได้รับข้อมูล และกรณีไม่ผ่านการคัดเลือกจะเก็บข้อมูลไว้ 2 ปี
	ระบบ File Server	
ข้อมูลผู้มาฝึกอบรมภายในกรมประชาสัมพันธ์	กระดาษ	10 ปี (กรณีเป็นเอกสารลับ 15 ปี) นับจากวันที่จัดเก็บเอกสาร
	ระบบ File Server	
	ระบบ WIFI Controller (Server ClearPass)	90 วัน หลังจากหมดเวลาการอนุญาตให้ใช้งาน
ข้อมูลการจัดกิจกรรม	กระดาษ	ตลอดระยะเวลาการดำเนินกิจกรรมของ กปส. และจัดเก็บไว้ในฐานข้อมูลไม่เกิน 2 ปี
	ระบบ File Server	
ข้อมูลการจัดทำและเผยแพร่หนังสือหมายเหตุ	กระดาษ	ตลอดระยะเวลาการดำเนินกิจกรรมของ กปส. และจัดเก็บไว้ในฐานข้อมูลไม่เกิน 2 ปี
ข้อมูลสื่อมวลชน	กระดาษ	ตลอดระยะเวลาการดำเนินกิจกรรมของ กปส. และจัดเก็บไว้ในฐานข้อมูลไม่เกิน 2 ปี
	ระบบ File Server	
CCTV's Data	ระบบ CCTV	2 ปี

ตาราง 1 ตัวอย่างการกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

หลักการทำข้อมูลนิรนาม (Anonymization)

แนวทางในการทำลายข้อมูลส่วนบุคคลแบ่งออกเป็น 2 วิธีดังนี้

1. ทำลายสื่อที่ใช้เก็บบันทึกข้อมูลส่วนบุคคล
2. การจัดทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization)

การจัดทำข้อมูลนิรนามคือกระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (negligible risk) โดยวิธีที่ได้รับความนิยมในการทำข้อมูลนิรนามมีดังนี้

- **[Scrambling]** การผสมข้อมูล เป็นการสลับลำดับของตัวอักษรในข้อมูลด้วยกฎเกณฑ์หนึ่ง ๆ อาทิ กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุกช่องข้อมูล ยกตัวอย่างเช่น 012345 กลายเป็น 210345 เป็นต้น
- **[Masking]** การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูล เช่น ข้อมูลหมายเลขโทรศัพท์ 0987654321 แสดงเป็น ######4321
- **[Blurring or Noising]** การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนั้นทวีความนิยมมากขึ้นในภาครัฐ ภาคเอกชนทั่วโลก เช่น มีชุดข้อมูลเป็น สีรถและทะเบียนรถ อาจจะลดข้อมูลเหลือ สีรถ
- **[Pseudonymization]** การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมา
- **[De-identification]** การขจัดตัวตน คือการลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่ เป็นการป้องกันการย้อนรอยเพื่อระบุตัวตน (re-identification) โดยพิจารณาถึงตัวข้อมูลเป็นหลัก ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย เช่น มีชุดข้อมูล ชื่อ นายจอห์น อีเมล์ john@example.com เบอร์โทร 0987654321 แสดงเป็น นาย A อีเมล - เบอร์โทร -

แนวทางการลบทำลายข้อมูลส่วนบุคคล

1. ขั้นตอนการลบทำลายข้อมูลส่วนบุคคล

1. หลักเกณฑ์ในการเริ่มต้นกระบวนการ
    - เมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
    - เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้มีการทำลายข้อมูลส่วนบุคคล
2. ขั้นตอนการปฏิบัติงาน

    2.1 คณะทำงานข้อมูลส่วนบุคคลขออนุญาตทำลายข้อมูลส่วนบุคคลที่ครบกำหนดหรือเจ้าของข้อมูลส่วนบุคคลมีการร้องขอให้ทำลายอย่างเป็นลายลักอักษรพร้อมทั้งระบุเหตุผลการทำลายและวิธีการที่จะใช้ในการทำลายข้อมูลส่วนบุคคล

    2.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการพิจารณา และอนุมัติในการทำลายข้อมูล
    - กรณีให้ทำลาย ให้ดำเนินการต่อในข้อ 2.3
    - กรณีที่ไม่ให้ทำลายให้สิ้นสุดกระบวนการ

    2.3 คณะทำงานข้อมูลส่วนบุคคลดำเนินการทำลายข้อมูลส่วนบุคคลตามแนวทางในการทำลายข้อมูลส่วนบุคคล

    2.4 คณะทำงานข้อมูลส่วนบุคคลบันทึกหลักฐานการทำลายข้อมูลส่วนบุคคล

    2.5 คณะทำงานข้อมูลส่วนบุคคลแจ้งผลการทำลายข้อมูลส่วนบุคคลกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

2. แนวทางการลบทำลายข้อมูลส่วนบุคคล

ประเภทสื่อที่ใช้เก็บ	การทำลายบันทึกข้อมูล	Anonymization
เอกสาร	• ใช้เครื่องย่อยเอกสาร • เผาทำลาย	Masking
เอกสาร electronic	ลบออกจากไดรฟ์เครือข่ายและล้างถังรีไซเคิลเป็นประจำ	
CD, DVD	ใช้เครื่องทำลาย CD/DVD หรือ หักทำลายเป็นส่วน ๆ อย่างน้อย 4 ส่วน	-
Thumb drive	ถอดแยกชิ้นส่วน และทำลายแผงวงจรภายในจนไม่สามารถประกอบใช้งานได้	• Masking • Scrambling • Blurring or noising • Pseudonymization

ประเภทสื่อที่ใช้เก็บ	การทำลายบันทึกข้อมูล	Anonymization
		• De-identification เช่น การลบข้อมูล หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์
Hard disk ประเภทจานหมุน	ทำให้แผ่นเก็บข้อมูลภายในเป็นรอยขีดข่วนร้ายแรง (ทุบ เจาะ บดขยี้) หรือ ใช้เครื่องทำลายแบบ Degaussing	• Masking • Scrambling • Blurring or noising • Pseudonymization • De-identification เช่น การลบข้อมูล หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์
Hard disk ประเภท SSD	ถอดแยกชิ้นส่วน และทำลายแผงวงจรภายในจนไม่สามารถประกอบใช้งานได้ (ทุบ เจาะ บดขยี้) หรือ ใช้เครื่องทำลายแบบ Degaussing	• Masking • Scrambling • Blurring or noising • Pseudonymization • De-identification เช่น การลบข้อมูล หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์

ตาราง 2 ตัวอย่างแนวทางการลบทำลายข้อมูลส่วนบุคคล

3. การจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล

กรณีองค์กรมีการจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล ต้องมีการกำกับและควบคุมกระบวนการระหว่างการทำลาย และเก็บรวบรวมหลักฐานการทำลายข้อมูลส่วนบุคคลจากผู้ให้บริการภายนอก