



นโยบายระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
และการลบหรือทำลายข้อมูลส่วนบุคคล
เมื่อพ้นกำหนดเวลา
(Data Retention Policy and Data Disposal Policy)

กรมการปกครอง

สารบัญ

๑. ข้อกำหนดทั่วไปของนโยบาย	หน้า
๑.๑ วัตถุประสงค์	๓
๑.๒ ขอบเขตของนโยบาย	๓
๑.๓ การยกเว้นการไม่ปฏิบัติตามนโยบาย	๓
๑.๔ กฎหมาย กฎเกณฑ์ และนโยบายที่เกี่ยวข้อง	๔
๑.๕ วันที่มีผลบังคับใช้	๔
๑.๖ ความถี่ในการทบทวน	๔
๑.๗ การทบทวนนโยบาย	๔
๑.๘ ผู้รับผิดชอบนโยบาย	๔
๒. ข้อกำหนดหลักของนโยบาย	
๒.๑ คำนิยาม	๔
๒.๒ หลักการทั่วไป	๕
๒.๓ บทบาท หน้าที่ และความรับผิดชอบ	๖
๒.๔ ข้อกำหนด	๖
๒.๕ บทกำหนดโทษ	๑๐
๒.๖ บทเฉพาะกาล	๑๑

แนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๓ วรรค ๓ ข้อมูลส่วนบุคคลที่จะมีการเก็บ รวบรวม และระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนด ระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม และมาตรา ๓๗ วรรค ๓ ระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลา การเก็บรักษา

แนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคลนี้จัดทำขึ้น เพื่อเป็นแนวทางในการกำกับข้าราชการ พนักงาน และลูกจ้างของกรมการปกครองและผู้ให้บริการภายนอกที่เกี่ยวข้องในการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคลที่กรมการปกครองมีการเก็บรวบรวม ใช้ หรือเปิดเผยตามภารกิจและการดำเนินงานให้มีความมั่นคงปลอดภัยและสอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑. ข้อกำหนดทั่วไปของนโยบาย

๑.๑ วัตถุประสงค์

แนวทางฉบับนี้มีวัตถุประสงค์เพื่อใช้ในการกำหนดขั้นตอนกระบวนการปฏิบัติการเก็บรักษาข้อมูลส่วนบุคคล และกระบวนการทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดการเก็บรักษา และไม่มีเมื่อนำข้อมูลกลับมาประมวลผล หรือเมื่อเจ้าของข้อมูลมีการร้องขอให้ทำลายข้อมูล

๑.๒ ขอบเขตของนโยบาย

นโยบายฉบับนี้ครอบคลุมกรมการปกครอง จะต้องนำนโยบายฉบับนี้ไปเป็นแนวทางในการจัดทำระเบียบ หลักเกณฑ์ และขั้นตอนการปฏิบัติงาน เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

๑.๓ การยกเว้นการไม่ปฏิบัติตามนโยบาย

ไม่มีข้อยกเว้นการไม่ปฏิบัติตามนโยบาย

๑.๔ กฎหมาย กฎเกณฑ์ และนโยบายที่เกี่ยวข้อง

นโยบายฉบับนี้เป็นไปตามกฎหมายและกฎเกณฑ์ดังต่อไปนี้ และให้หมายความรวมถึงกฎหมายและกฎเกณฑ์ ที่เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในที่นี้ด้วย

๑.๔.๑ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๔.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒

๑.๔.๓ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล" เรื่อง หลักเกณฑ์และวิธีการแจ้งเหตุการรั่วไหลของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๑.๔.๔ กฎหมาย กฎเกณฑ์ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง (ถ้ามี)

๑.๕ วันที่มีผลบังคับใช้

ประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

๑.๖ การทบทวนแนวทาง

กรมการปกครองจะดำเนินการทบทวนแนวทางนี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และเมื่อพิจารณาปรับปรุง แก้ไข หรือเปลี่ยนแปลงแนวทางนี้ตามที่เห็นสมควรแล้ว จะทำการแจ้งให้ท่านได้รับทราบผ่านช่องทางเว็บไซต์ dpo@dopa.go.th โดยการระบุวันที่กำกับไว้ที่แนวทาง ปค. จึงขอแนะนำให้ท่านตรวจสอบเพื่อรับทราบแนวทางฉบับใหม่อย่างสม่ำเสมอ

๑.๗ ผู้รับผิดชอบนโยบาย

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และคณะทำงานฯ เป็นผู้รับผิดชอบและบังคับใช้นโยบายฉบับนี้

๒. ข้อกำหนดหลักของนโยบาย

๒.๑ คำนิยาม

“บุคลากร” หมายถึง หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง เจ้าหน้าที่ของรัฐ และผู้ที่ได้มอบหมายให้ปฏิบัติหน้าที่ ของกรมการปกครอง

“ปค.” หมายถึง กรมการปกครอง

“คณะกรรมการกำกับดูแล ฯ” หมายถึง คณะกรรมการกำกับดูแลการดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประจำปีกรมการปกครอง ที่ได้รับการแต่งตั้งตามคำสั่งของกรมการปกครอง

“คณะทำงาน ฯ” หมายถึง คณะทำงานเพื่อขับเคลื่อนการดำเนินการตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่ได้รับการแต่งตั้งตามคำสั่งของกรมการปกครอง

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่กรมการปกครอง เก็บรวบรวม ใช้ หรือเปิดเผย

“กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” หรือ “พ.ร.บ.ฯ” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม รวมถึงประกาศ กฎระเบียบ และกฎหมายอื่นใดที่ออกตามพระราชบัญญัติ ดังกล่าว

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคล ซึ่งกระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจาก อำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อการกระทำโดย ปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

“การรั่วไหลของข้อมูลส่วนบุคคล” (Personal Data Breach) หมายถึง เหตุการณ์ที่ส่งผลให้ข้อมูลส่วนบุคคลถูกเข้าถึงโดยมิชอบ สูญหาย ถูกเปิดเผยโดยไม่ได้รับอนุญาต หรือถูกใช้งานผิดวัตถุประสงค์ ซึ่งส่งผลกระทบต่อความมั่นคง ความลับ และสิทธิของเจ้าของข้อมูลส่วนบุคคล”

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลอ่อนไหว” หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“ข้อมูลชีวภาพ” (Biometric Data) หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้อง กับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ ทำให้สามารถยืนยันตัวตนของบุคคลนั้น ที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

“เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล ที่กรรมการปกครอง เก็บรวบรวม ใช้ หรือเปิดเผย

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer -DPO) หมายถึง ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงาน ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“ระยะเวลาการเก็บรักษา” หมายความว่า ช่วงเวลาที่เหมาะสมที่กรรมการปกครองพิจารณาเห็นสมควรให้มีการเก็บรักษาข้อมูลส่วนบุคคลเหล่านั้นไว้เพื่อประโยชน์ในการประมวลผลข้อมูลส่วนบุคคลซึ่งต้องสอดคล้องตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล โดยจะจัดเก็บไว้เป็นระยะเวลาหนึ่งตามความจำเป็นเท่านั้น

“การลบทำลาย” หมายความว่า การทำให้ข้อมูลส่วนบุคคลไม่สามารถบ่งชี้กลับมายังตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้อีก โดยอาศัยวิธีการลบทำลายต่างๆ ที่เหมาะสมตามชนิดหรือรูปแบบของการจัดเก็บข้อมูล

๒.๒ หลักการทั่วไป

กรรมการปกครองอาจเก็บรวบรวมหรือได้มาซึ่งข้อมูลดังต่อไปนี้ ซึ่งอาจรวมถึงข้อมูลส่วนบุคคลของท่าน ทั้งนี้ ขึ้นอยู่กับงานบริการที่ท่านขอรับบริการหรือบริบทความสัมพันธ์ที่ท่านมีกับกรรมการปกครอง รวมถึงข้อพิจารณาอื่นที่มีผลกับการเก็บรวบรวมข้อมูลส่วนบุคคล โดยประเภทของข้อมูลที่ระบุไว้ดังต่อไปนี้ เป็นเพียงกรอบการเก็บรวบรวมข้อมูลส่วนบุคคลของกรรมการปกครองเป็นการทั่วไป ทั้งนี้ เฉพาะข้อมูลที่เกี่ยวข้องกับบริการที่ท่านใช้งานหรือมีความสัมพันธ์ด้วยเท่านั้นที่จะมีผลบังคับใช้

๑. ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลระบุชื่อเรียกของท่านหรือข้อมูลจากเอกสารราชการที่ระบุข้อมูลเฉพาะตัวของท่าน เช่น คำนำหน้าชื่อ ชื่อ นามสกุล ชื่อกลาง ชื่อเล่น ลายมือชื่อ เลขที่บัตรประจำตัวประชาชน สัญชาติ เลขที่ใบขับขี่ เลขที่หนังสือเดินทาง ข้อมูลทะเบียนบ้าน หมายเลขใบประกอบการ หมายเลขใบอนุญาตการประกอบวิชาชีพ (สำหรับแต่ละอาชีพ) หมายเลขประจำตัวผู้ประกันตน หมายเลขประกันสังคม เป็นต้น

๒. ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ได้แก่ ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนของท่าน เช่น เชื้อชาติ ข้อมูลศาสนา ข้อมูลความพิการ ข้อมูลความเห็นทางการเมือง ประวัติอาชญากรรม ข้อมูลชีวภาพ (ข้อมูลภาพจำลองใบหน้า) ข้อมูลพันธุกรรม ข้อมูลเกี่ยวกับสุขภาพ เป็นต้น ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ให้ข้อมูลที่มีความจำเป็นในการให้บริการของ กรรมการปกครอง อาจเป็นผลให้กรรมการปกครอง ไม่สามารถให้บริการนั้นแก่เจ้าของข้อมูลส่วนบุคคลดังกล่าวได้ทั้งหมดหรือบางส่วน

๒.๓ บทบาท หน้าที่ และความรับผิดชอบ

๒.๓.๑ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๒ เจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

๑) ให้คำแนะนำ แก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

๒) ตรวจสอบ การดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

๓) ประสานงานและให้ความร่วมมือ กับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้

๔) รักษาความลับของข้อมูลส่วนบุคคล ที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

๒.๓.๒ คณะกรรมการกำกับดูแล ๗/ บุคลากร

บุคลากรทุกคน มีหน้าที่ต้องปฏิบัติตามนโยบายฉบับนี้และคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคลของกรมการปกครอง ทั้งนี้คณะกรรมการกำกับดูแลการดำเนินการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประจํากรมการปกครอง และหน่วยงาน มีหน้าที่รับผิดชอบในการกำหนดหรือปรับปรุง นโยบาย ระเบียบปฏิบัติงาน และ/หรือคู่มือปฏิบัติงานที่เกี่ยวข้อง เพื่อให้สอดคล้องกับหลักการ ตามแนวนโยบายฉบับนี้ ตลอดจนกำหนดให้มีการกำกับดูแลบุคลากรให้ปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๔ ข้อกำหนด

๒.๔.๑ แนวทางในการดำเนินการเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดเวลา กรมการปกครอง กำหนดแนวทางดังต่อไปนี้

ก. กรมการปกครองจะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย โดยกรมการปกครองจะขอ ความยินยอม โดยชัดแจ้งจากท่านก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลของท่านตามวัตถุประสงค์

ข. กรมการปกครอง จะลบหรือทำลายข้อมูลส่วนบุคคลที่ไม่มีจำเป็นต่อการประมวลผลข้อมูลส่วนบุคคล ตามวัตถุประสงค์ หรือไม่มีเหตุตามกฎหมายที่จะต้องเก็บรักษาข้อมูลส่วนบุคคล เพื่อปฏิบัติ ตามกฎหมาย หรือมีกฎหมายเฉพาะเจาะจงกำหนดให้กรมการปกครอง มีหน้าที่หรือมีสิทธิในการเก็บรักษา ข้อมูลส่วนบุคคลต่อไป

ค. กรรมการปกครอง จะจัดให้มีระบบตรวจสอบการเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล เพื่อให้ เกิดความมั่นใจว่าจะไม่มีการปฏิบัติผิดกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยจะมี การทบทวนการเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดเวลา อย่างน้อย ปีละ ๑ ครั้ง

๒.๔.๒ การเก็บรักษาข้อมูลส่วนบุคคล กรรมการปกครอง เก็บรักษาข้อมูลส่วนบุคคลของท่าน ดังต่อไปนี้

ก. ข้อมูลส่วนบุคคลของท่าน ไม่ว่าจะเก็บรักษาในรูปแบบกระดาษ หรือรูปแบบดิจิทัล จะถูกจัดการ ให้มีความมั่นคงปลอดภัยตามนโยบายฯ อย่างเคร่งครัด

ข. กรรมการปกครอง จะมีระบบตรวจสอบการเก็บรักษาข้อมูลส่วนบุคคล ไม่ว่าจะจัดเก็บในตู้เก็บเอกสาร คอมพิวเตอร์ อุปกรณ์ที่สามารถจัดเก็บข้อมูลในรูปแบบดิจิทัล โทรศัพท์มือถือ และในระบบ Cloud อย่างสม่ำเสมอ และให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของกรรมการปกครอง และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๒.๔.๓ กำหนดเวลาในการเก็บรักษาข้อมูลส่วนบุคคล และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

ลำดับ	ประเภทหรือรายการข้อมูลส่วนบุคคล	ประเภทข้อมูลส่วนบุคคล	แหล่งข้อมูล	หน่วยงานภายใน	วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผย	ระยะเวลาเก็บรักษา
๑						
๒						
๓						

๒.๔.๔ การลบหรือทำลายข้อมูลส่วนบุคคล กรรมการปกครอง จะลบหรือทำลายข้อมูลส่วนบุคคลของท่าน ดังต่อไปนี้

๒.๔.๔.๑ เมื่อครบกำหนดเวลาเก็บรักษาข้อมูลส่วนบุคคล หรือเมื่อกรรมการปกครอง เห็นด้วยกับการร้องขอให้ลบ หรือทำลายข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคล

๒.๔.๔.๒ หน่วยงานภายในกรรมการปกครอง จะต้องทำหนังสือขออนุญาตลบหรือทำลาย พร้อมระบุเหตุผล และวิธีการที่จะใช้ดำเนินการส่งถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อพิจารณาอนุมัติ หรือปฏิเสธการอนุมัติ

๒.๔.๔.๓ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะพิจารณาแนวทางการทำลาย โดยว่าจ้างผู้เชี่ยวชาญ เพื่อให้มาดำเนินการโดยอาจจะเป็นการทำลายสิ่งที่ใช้เก็บข้อมูลส่วนบุคคล หรือการจัดทำให้ ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม (Anonymization) เพื่อลดความเสี่ยงจากการใช้ข้อมูล ส่วนบุคคล โดยมีขอบหรือการรั่วไหลของข้อมูลส่วนบุคคล ซึ่งปัจจุบันมีวิธีการทำให้เป็นข้อมูลนิรนาม ดังนี้

ก. [Scrambling] การผสมข้อมูล เป็นการสลับลำดับของตัวอักษรในข้อมูล ด้วยกฎเกณฑ์ หนึ่ง เช่น กำหนดกฎเกณฑ์ว่าให้สลับตัวอักษรตัวแรกกับตัวที่สามของทุกช่องข้อมูล ยกตัวอย่างเช่น ๐๑๒๓๔๕ กลายเป็น ๒๑๐๓๔๕ เป็นต้น

ข. [Masking] การปิดทับข้อมูล การเปลี่ยนส่วนใดส่วนหนึ่งของข้อมูลส่วนบุคคล เช่น ข้อมูลบัตรประชาชน และหมายเลขบัตรประจำตัวประชาชน ตัวอย่าง xxxx (๔x) สี่ตัวท้ายหมายเลขบัตรประจำตัวประชาชน ๑๒๓๔๕๖๗๘๙xxxx ข้อมูลหมายเลขโทรศัพท์ ตัวอย่าง ๐๘๙๕๕๕๕xxxx

ค. [Blurring or Noising] การลดความชัดเจนของข้อมูลลง เป็นการใช้ข้อมูลโดยประมาณ แทนที่ข้อมูลดั้งเดิม เพื่อลดความเฉพาะเจาะจงของข้อมูลลง วิธีดังกล่าวนี้ทวีความนิยม มากขึ้นในภาครัฐ ภาคเอกชนทั่วโลก เช่น มีชุดข้อมูล เป็น สีรและทะเบียนรถ อาจจะลด ข้อมูลเหลือเพียง สีรถ

ง. [Pseudonymization] การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตน ของเจ้าของข้อมูลโดยตรง เช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัส ที่สร้างขึ้น

จ. [De-identification] การจัดตัวตน คือ การลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตน ใหม่ เป็นการป้องกันการย้อนรอยเพื่อระบุตัวตน (re-identification) โดยพิจารณาถึงตัว ข้อมูลเป็นหลัก ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย เช่น มีชุดข้อมูล ชื่อ นายจอห์น อีเมล john@example.com เบอร์โทร ๐๙๐๑๑๑๑๑๑๑๑๑๑๑ แสดงเป็น นาย A อีเมล – เบอร์โทร

๒.๔.๕ แนวทางการลบทำลายข้อมูลส่วนบุคคล

๑) ขั้นตอนการลบทำลายข้อมูลส่วนบุคคล

๑.๑) หลักเกณฑ์ในการเริ่มต้นกระบวนการ

- เมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้มีการทำลายข้อมูลส่วนบุคคล

๑.๒) ขั้นตอนการปฏิบัติงาน

๑.๒.๑. คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) ขออนุญาตทำลายข้อมูลส่วนบุคคลที่ครบกำหนดหรือเจ้าของ ข้อมูลส่วนบุคคลมีการร้องขอให้ทำลายอย่างเป็นลายลักษณ์อักษรพร้อมทั้งระบุเหตุผลการทำลาย และวิธีการที่จะใช้ในการทำลายข้อมูลส่วนบุคคล

๑.๒.๒. ผู้บริหารหน่วยงาน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการพิจารณา และอนุมัติในการทำลายข้อมูล

- กรณีให้ทำลาย ให้ดำเนินการต่อในข้อ ๑.๒.๓
- กรณีที่ไม่ให้ทำลายให้สิ้นสุดกระบวนการ

๑.๒.๓. คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) ดำเนินการทำลายข้อมูลส่วนบุคคลตามแนวทางในการทำลาย ข้อมูลส่วนบุคคล

๑.๒.๔. คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) บันทึกหลักฐานการทำลายข้อมูลส่วนบุคคล

๑.๒.๕. คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) แจ้งผลการทำลายข้อมูลส่วนบุคคลกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๒) แนวทางการลบทำลายข้อมูลส่วนบุคคล

ที่	ประเภทสื่อที่จัดเก็บข้อมูล	การลบทำลายข้อมูล
๑	บนกระดาษ	- ทำลายด้วยเครื่องทำลายเอกสาร ที่ไม่สามารถนำซากเอกสารที่ทำลายแล้วมาประกอบและอ่านข้อมูลได้ หรือตามกฎหมาย ว่าด้วยงานสารบรรณกำหนด
๒	ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ ของ ปค.	- ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ปค. กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ - ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
๓	บนเครื่องให้บริการ หรือฐานข้อมูลของระบบสารสนเทศต่างๆ	- ใช้คำสั่งการลบทำลาย (delete) ของระบบบริหารจัดการฐานข้อมูล - ใช้คำสั่งการลบทำลาย (delete) เครื่องให้บริการระบบ (Virtual Machine) ที่ควบคุมการเข้าถึงข้อมูลนั้น - ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
๔	บนสื่อบันทึกข้อมูลประเภทฮาร์ดดิสก์	- ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ปค. กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ เช่น • Hard disk ประเภทจานหมุน ทำให้แผ่นเก็บข้อมูลภายในเป็นรอยขีดข่วน ร้ายแรง (ทุบ เจาะ บดขยี้) หรือ ใช้เครื่องทำลายแบบ Degaussing หรือ De-identification • Hard disk ประเภท SSD ถอดแยกชิ้นส่วน และทำลายแผงวงจร ภายในจนไม่สามารถประกอบใช้งานได้ (ทุบ เจาะ บดขยี้) หรือ ใช้เครื่องทำลายแบบ Degaussing หรือ De-identification - ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
๕	บนสื่อบันทึกข้อมูลประเภทเคลื่อนที่ได้	- ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ปค. กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูลการลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ อาทิ • ใช้เครื่องทำลาย CD/DVD หรือหักทำลายเป็นชิ้นๆ อย่างน้อย ๔ ส่วน • Thumb drive ถอดแยกชิ้นส่วน และทำลายแผงวงจร ภายในจนไม่สามารถประกอบใช้งานได้ หรือ De-identification - ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ที่	ประเภทสื่อที่จัดเก็บข้อมูล	การลบทำลายข้อมูล
๖	บนคลาวด์	- ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ปค. กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูล การลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ - ใช้คำสั่งการลบทำลาย (delete) เครื่องให้บริการระบบ (Virtual Machine) ที่ควบคุมการเข้าถึงข้อมูลนั้น (ในกรณีที่เป็นการใช้บริการคลาวด์ ที่อนุญาตให้มีการสร้างเครื่องให้บริการได้ และไม่มีการใช้งานเครื่อง ให้บริการนั้นอีกต่อไป) - ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

๓) การจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล

กรณีที่มีการจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล ต้องมีการกำกับ และควบคุมกระบวนการ การระหว่งการทำลาย และเก็บรวบรวมหลักฐานการทำลายข้อมูลส่วนบุคคลจากผู้ให้บริการภายนอก และดำเนินการตามกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๒.๔.๖ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กรมการปกครอง ได้ดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และจัดให้มีคณะทำงาน ฯ เพื่อสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามหน้าที่ของกรมการปกครอง ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ)

อีเมล : dpo@dopa.go.th

โทรศัพท์ : ๐๒-๘๒๘-๑๐๔๗

ทั้งนี้ คณะทำงานฯ จะช่วยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการตรวจสอบการดำเนินการของกรมการปกครอง ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และทำหน้าที่รับผิดชอบในการพิจารณาคำร้องขอใช้สิทธิ ของเจ้าของข้อมูลส่วนบุคคลก่อนดำเนินการตามคำร้องขอ พร้อมการแจ้งผลการปฏิบัติตามคำขอ ใช้สิทธิให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า รวมถึงต้องจัดให้มีการบันทึกการจัดการ ข้อมูลส่วนบุคคล กรณีที่มีการปฏิเสธคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อใช้เป็น หลักฐานเมื่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล ร้องขอ

๒.๕ บทกำหนดโทษ

หากผู้บริหารหรือบุคลากรของกรมการปกครอง และ/หรือผู้ปฏิบัติงานตามสัญญา กับกรมการปกครอง ละเลย หรือละเว้นไม่สั่งการ หรือไม่ดำเนินการ หรือสั่งการ หรือดำเนินการอย่างใดอย่างหนึ่งในหน้าที่ของตนอันเป็นการฝ่าฝืนนโยบายฯ หรือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กรมการปกครอง จะจัดให้มีการสอบสวนข้อเท็จจริง และดำเนินการ ลงโทษทางวินัยอย่างจริงจัง

๒.๖ บทเฉพาะกาล

นโยบาย ระเบียบปฏิบัติ คู่มือปฏิบัติงานใดที่ไม่ขัดหรือแย้ง หรือมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เข้มข้นกว่า นโยบายฉบับนี้ให้มีผลใช้บังคับต่อไป แต่หากปรากฏว่ามีข้อความใดขัดหรือแย้งกับนโยบายฉบับนี้ หรือมี มาตรการต่ำกว่ามาตรการที่กำหนดไว้ในนโยบายฉบับนี้ ให้คณะทำงานฯ สนับสนุนการทำงานของเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะดำเนินการแก้ไขให้เสร็จสิ้นภายใน ๖๐ วัน