



กระบวนการตรวจสอบฐานทางกฎหมายในการจัดเก็บข้อมูลส่วนบุคคล

ดย. มีแนวปฏิบัติในการพิจารณาฐานแห่งการประมวลผลข้อมูลส่วนบุคคล โดยจำแนกออกเป็น ๗ ฐานได้แก่

๑. ความยินยอม
๒. ประโยชน์สำคัญต่อชีวิต
๓. สัญญา
๔. กิจสาธารณะ/อำนาจรัฐ
๕. ประโยชน์อันชอบด้วยกฎหมาย
๖. ปฏิบัติหน้าที่ตามกฎหมาย
๗. จดหมายเหตุ/วิจัย/สถิติ

การพิจารณาฐานแห่งการประมวลผลเป็นสิ่งที่ย. ให้มีความสำคัญในการประมวลผลข้อมูลส่วนบุคคลเป็นอย่างมาก เพราะฐานแห่งการประมวลผลเป็นสิ่งกำหนดแนวปฏิบัติอื่น ๆ ของการคุ้มครองข้อมูลส่วนบุคคลรวมถึงสิทธิพึงมีของเจ้าของข้อมูลส่วนบุคคลด้วย โดยแนวปฏิบัติในการพิจารณาฐานแห่งการประมวลผลข้อมูลส่วนบุคคล อ้างอิงแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

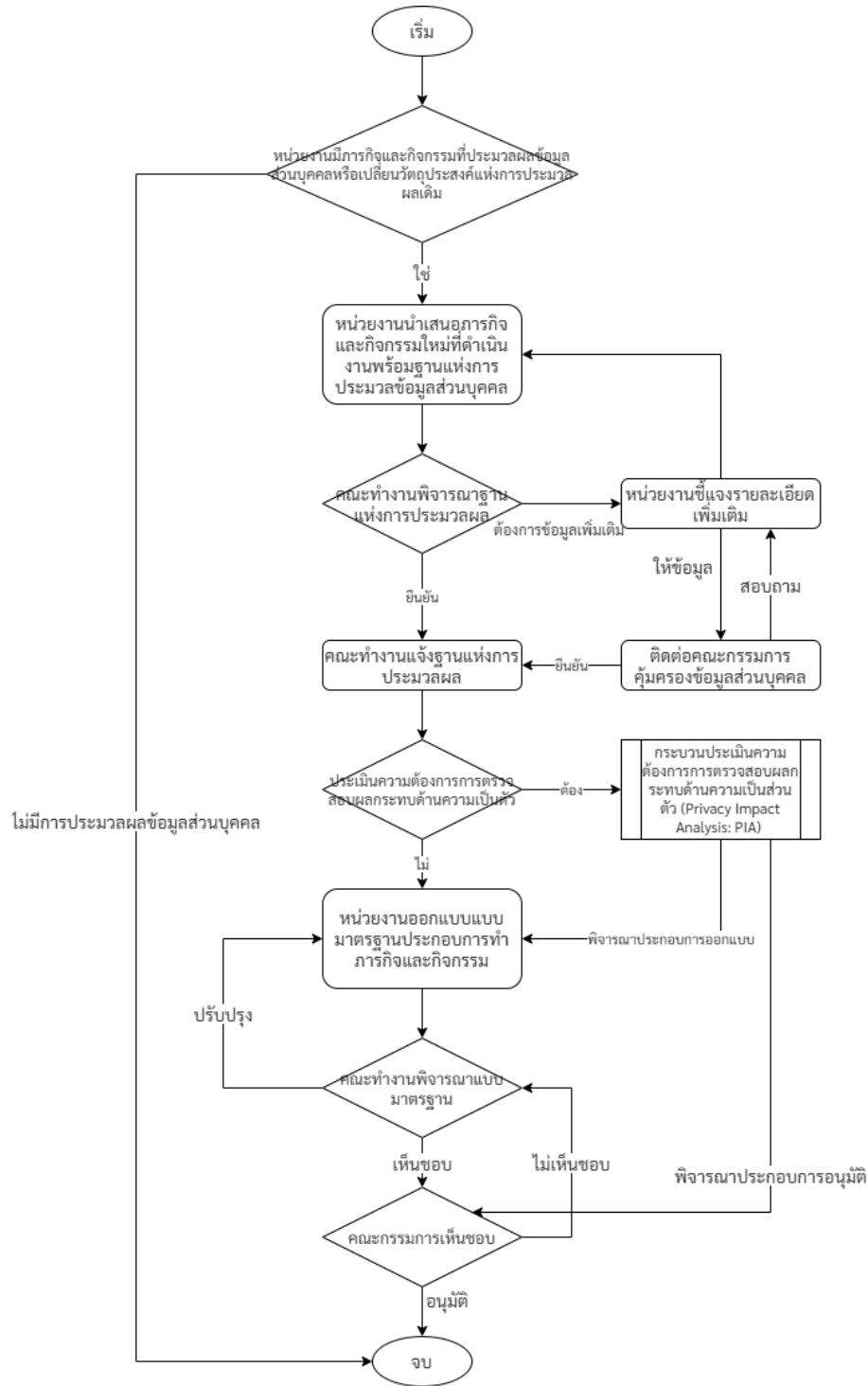
การพิจารณาฐานแห่งการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลมีกระบวนการตามที่ปรากฏ โดยสรุปสาระสำคัญของกระบวนการดังนี้

- ❖ กระบวนการพิจารณาฐานแห่งการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล ถูกใช้เมื่อมีการดำเนินกิจกรรมตามภารกิจของหน่วยงานใหม่ หรือมีการเปลี่ยนแปลงวัตถุประสงค์เดิมของภารกิจและกิจกรรมเดิม ที่เกี่ยวข้องกับประมวลผลข้อมูลส่วนบุคคล ซึ่งต้องได้รับการออกแบบเอกสารต่างๆ อาทิ แบบมาตรฐาน คำแถลงความเป็นส่วนตัว นโยบายการคุ้มครองข้อมูลส่วนบุคคล สิทธิของผู้เป็นเจ้าของข้อมูล ระยะเวลาการจัดเก็บ มาตรการด้านความมั่นคงปลอดภัยที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล รายการไหลของข้อมูลและบัญชีข้อมูลส่วนบุคคล รายงานผลกระทบด้านความเป็นส่วนตัว ตลอดจนช่องทางติดต่อ และได้รับการตรวจทานจากคณะกรรมการอนุมัติโดยคณะกรรมการ
- ❖ ผลลัพธ์ของกระบวนการที่สำคัญคือการกำหนดฐานแห่งการประมวลผลข้อมูลส่วนบุคคลในภารกิจกิจกรรม หรือวัตถุประสงค์นั้นๆ โดยได้ไตร่ตรองถึงความจำเป็นในการใช้ข้อมูลส่วนบุคคล รวมถึงทางเลือก (หากมี) ที่จะไม่ประมวลผลข้อมูลส่วนบุคคลแต่ยังสามารถดำเนินการให้บริการสู่เป้าประสงค์ได้เช่นกัน
- ❖ กรณีเกิด ความคลุมเครือ ไม่ชัดเจน ในการกำหนดฐานแห่งการประมวลผลข้อมูลส่วนบุคคล คณะทำงานต้องพิจารณาชี้แจงและสอบถามถึงคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้คณะกรรมการคุ้มครองข้อมูล



ส่วนบุคคลสรุปและให้คำแนะนำในการกำหนดฐานแห่งการประมวลผลข้อมูลส่วนบุคคลของ ภารกิจ กิจกรรม หรือวัตถุประสงค์นั้น ๆ

- ❖ อนึ่ง หากมีกระบวนการใด ๆ ภายใต้ภารกิจหรือกิจกรรมใด ๆ ในการกำกับดูแลของ ดย. ที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ต้องมีอย่างน้อย 1 ฐานแห่งการประมวลผล กล่าวอีกนัยคือจะไม่มีข้อมูลส่วนบุคคลใด ๆ ใน ดย. ที่ได้มาโดยปราศจากฐานแห่งการประมวลผล



ภาพที่ ๑ กระบวนการพิจารณาฐานแห่งการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล



นิยามและคำสำคัญ

คำสำคัญ	หมายถึง
เจ้าหน้าที่	เจ้าหน้าที่พนักงาน ข้าราชการ หรือพนักงานราชการ ตลอดจนหน่วยงานภายนอกที่กระทำการใด ๆ ในฐานะของ ดย.
คณะทำงาน	คณะทำงานคุ้มครองข้อมูลส่วนบุคคล กรมกิจการเด็กและเยาวชน
คณะกรรมการ	คณะกรรมการกำกับดูแลข้อมูล กรมกิจการเด็กและเยาวชน / คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กรมกิจการเด็กและเยาวชน
แบบมาตรฐาน	แบบฟอร์ม หรือ ระบบสารสนเทศ ที่เป็นมาตรฐานใช้ในการปฏิบัติการกิจของ ดย.
หน่วยงาน	ดย. หน่วยงานภายใน ดย. และหน่วยงานภายนอกที่กระทำการใด ๆ ในฐานะ ดย. (outsourcing)

ฐานความยินยอม

ความยินยอมเป็นฐานในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลได้สมัครใจ “เลือก” ที่จะยินยอมให้ผู้ควบคุมข้อมูลประมวลผลได้ โดยหากต้องการใช้ความยินยอมเป็นฐานในการประมวลผล ผู้ควบคุมข้อมูลจะต้องเชิญชวนให้เจ้าของข้อมูลยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆ ได้ โดยมั่นใจว่าเป็นสถานการณ์ที่เจ้าของข้อมูลเลือกที่จะปฏิเสธได้จริง และหากเจ้าของข้อมูลเลือกที่จะปฏิเสธผู้ควบคุมข้อมูลก็ไม่สามารถประมวลผลได้ ความยินยอมจะต้องไม่เป็นเงื่อนไขในการรับบริการ หรือผูกติดอยู่กับความจำเป็นในการปฏิบัติ

ตามสัญญา การใช้ความยินยอมเป็นฐานในการประมวลผลจึงมักเกิดขึ้นในกรณีที่เป็นการเสริมจากบริการหลักซึ่งไม่ครอบคลุมตามสัญญา การใช้ฐานความยินยอมจึงต้องกระทำด้วยความระมัดระวัง อีกทั้ง ควรตระหนักว่าผู้ควบคุมข้อมูลจะมีการพิสูจน์ว่าเจ้าของข้อมูลนั้นได้เลือกที่จะยินยอมโดยสมัครใจจริงๆ และความยินยอมของเจ้าของข้อมูลไม่ใช่ใบอนุญาตให้ทำอะไรกับข้อมูลนั้นก็ได้ การประมวลผลข้อมูลบนฐานของความยินยอมยังต้องยึดตามหลักความจำเป็น และต้องทำให้เนื้อหาของข้อมูลถูกต้องด้วย

ด้วยลักษณะที่ยึดโยงอยู่กับความสมัครใจของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะต้องสอดคล้องกับเงื่อนไขที่กำหนดไว้ในมาตรา ๑๙ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ความยินยอมจึงเป็นฐานการประมวลผลที่มีความเสี่ยงมาก เพราะอาจต้องหยุดประมวลผลเมื่อใดก็ตามที่เจ้าของข้อมูลถอนความยินยอมไป ดังนั้น หากการประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อความจำเป็นในการปฏิบัติตามสัญญาโดยแท้จริง ไม่มีความจำเป็นใดๆ ที่จะต้องขอความยินยอมอีก

ดย. เป็นหน่วยงานภาครัฐที่ได้อำนาจในการดำเนินกิจการและบริการสาธารณะตามกฎหมาย ฉะนั้นการประมวลผลข้อมูลส่วนบุคคลบนฐานความยินยอมจึงมีโอกาสน้อยมากเว้นแต่เสียว่า

- ❖ การประมวลผลข้อมูลส่วนบุคคลนั้นนอกเหนือจากอำนาจของ ดย. ที่ได้ตามกฎหมาย
- ❖ การประมวลผลข้อมูลส่วนบุคคลนั้นเกินกว่าที่จำเป็นต้องใช้ แต่ ดย. ได้ตัดสินใจและประเมินผลกระทบในการประมวลผลข้อมูลประเภทนั้น
- ❖ การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นบริการเสริมเพื่อโครงการที่ ดย. ริเริ่มโดยไม่ได้เชื่อมโยงต่อหน้าที่และภารกิจหลักของหน่วยงาน
- ❖ การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ตกตามฐานการประมวลอื่น ๆ อีก ๖ ประเภท



แนวทางการใช้ฐานความยินยอม

- ❖ ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้
- ❖ เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่างๆ อย่างครบถ้วน แต่เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่น FAOS, pop-up screen, chatbot ที่ทำให้การให้ข้อมูลนั้นชัดเจนมากขึ้น การให้ข้อมูลอาจกระทำได้หลายรูปแบบ ทั้งข้อเขียน ปากเปล่า วิดีโอ ข้อความเสียง หรือข้อความอิเล็กทรอนิกส์ก็ได้ トラบใดที่ข้อมูลเหล่านั้นสามารถเข้าถึงได้ง่าย และมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่นๆ ผู้ควบคุมข้อมูลควรทดสอบด้วยว่าเนื้อหาสามารถอ่านเข้าใจได้ง่ายและไม่แตกต่างไปจากความคาดหมายปกติสำหรับคนทั่วไป อีกทั้งต้องคำนึงถึงอายุของผู้ให้ความยินยอมว่าภาษาที่ใช้ั้นเหมาะสมกับระดับความสามารถในการเข้าใจในบริบทนั้นๆ ด้วยหรือไม่ การอธิบายด้วยภาพเคลื่อนไหวหรือรูปภาพหรือ infographic เป็นที่นิยมเพราะสามารถช่วยอำนวยความสะดวกเข้าใจได้โดยเฉพาะในกรณีของการขอความยินยอมจากผู้เยาว์

เมื่อเจ้าหน้าที่ ได้พิจารณาเห็นแล้วว่าแบบมาตรฐานในการเก็บรวบรวมข้อมูลส่วนบุคคลของ ดย. แบบใด มีองค์ประกอบอันแสดงประจักษ์ถึงฐานความยินยอม เจ้าหน้าที่ต้องอธิบายให้เจ้าของข้อมูลทราบเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล วัตถุประสงค์ ระยะเวลาการเก็บข้อมูลส่วนบุคคล ตลอดจนสิทธิของเจ้าของข้อมูลส่วนบุคคล ก่อนการลงนาม อนุมัติ หรือส่งมอบข้อมูลส่วนบุคคล ในแบบมาตรฐานดังกล่าว

ในกรณีที่สถานการณ์ไม่อำนวยต่อการใช้แบบมาตรฐานในการเก็บรวบรวมข้อมูลส่วนบุคคล เจ้าหน้าที่ต้องอธิบายด้วยวิธีการใดๆ ที่วิญญูชนพึงเข้าใจได้โดยง่าย อาทิ การพูดอธิบาย การเขียน (สำหรับผู้พิการทางการได้ยิน)

เมื่อเจ้าของข้อมูลส่วนบุคคลปฏิเสธการให้ความยินยอม เจ้าหน้าที่ต้องชี้แจงและไม่กล่าวอ้างถึงการไม่ให้บริการหรือสร้างความเลื่อมล้ำ หรือดำเนินการใดๆ อันแสดงถึงพฤติกรรมที่สร้างความไม่เท่าเทียมและเลือกปฏิบัติต่อเจ้าของข้อมูลส่วนบุคคลรายนั้นหรือกลุ่มนั้น เจ้าหน้าที่ถึงระลึกเสมอว่าข้อมูลส่วนบุคคลที่ต้องเก็บรวบรวมบนฐานความยินยอมย่อมไม่กระทบต่ออำนาจและภารกิจของรัฐ อนึ่งเจ้าหน้าที่ย่อมไม่มีความผิดหรือบกร่องต่อหน้าที่หากไม่ได้มาซึ่งข้อมูลส่วนบุคคลนั้น

การเปิดเผยข้อมูลส่วนบุคคลที่ได้มาซึ่งฐานความยินยอม ต้องได้รับอนุมัติจากคณะกรรมการเท่านั้น ห้ามมิให้มีการเปิดเผยข้อมูลส่วนบุคคลกับผู้ไม่ใช่เจ้าของข้อมูลโดยเด็ดขาด แม้จะเป็นเครือญาติ พี่น้อง หรือมีความสัมพันธ์กับผู้เป็นเจ้าของข้อมูล เว้นแต่เสียว่ามีการกล่าวอ้างสิทธิโดยชอบที่กฎหมายอื่นได้กำหนดไว้ เจ้าหน้าที่ต้องรับมาพิจารณาและจัดส่งรายการคำขอดังกล่าวแก่คณะทำงานเพื่อพิจารณาต่อไป

- ❖ ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ ผู้ควบคุมข้อมูลจะไม่นำฐานความยินยอม (consent) กับฐานการปฏิบัติตามสัญญา (contract) มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น



ในบริบทของ ดย. ความยินยอมย่อมไม่กระทบต่อสิทธิของประชาชนที่พึงได้รับการสาธารณะจาก ดย. ภายใต้อำนาจและขอบเขตที่กฎหมายกำหนดให้บริการประชาชนแก่ ดย.

- ❖ ดย. ต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตนและแก่เจ้าของข้อมูลหากได้รับความยินยอม เช่น จะทำให้ประสบการณ์การใช้บริการสะดวกรวดเร็วยิ่งขึ้น ลดขั้นตอนและระยะเวลาในการตรวจสอบตัวตน เป็นต้น อีกทั้งการอธิบายเกี่ยวกับมาตรการที่จะช่วยสร้างความปลอดภัยให้กับข้อมูลที่ได้รับคามยินยอมให้ประมวลผลนั้นก็อาจช่วยทำให้เจ้าของข้อมูลมีความไว้วางใจ และยินยอมให้ประมวลผลข้อมูลได้ง่ายขึ้น

ในบริบทของ ดย. เจ้าหน้าที่ต้องชี้แจงประโยชน์ที่เกิดขึ้นจากการได้มาซึ่งความยินยอม โดยไม่กล่าวอ้างเกินจริง หรือสร้างความตระหนกตกใจ หรือพฤติกรรมใด ๆ ที่กระทบต่ออิสรภาพ เสรีภาพ ทาง การตัดสินใจและยินยอมของเจ้าของข้อมูล โดยเด็ดขาด

อนึ่งเพื่อเป็นมาตรฐานอันดี ให้หน่วยงานที่มีการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลบนฐานความยินยอม กำหนดลักษณะข้อความทั้งใน การเขียนลงสื่อ (ทั้งกระดาษและดิจิทัล) และการพูดชี้แจง เพื่อเป็นแนวปฏิบัติให้แก่เจ้าหน้าที่ที่ต้องเข้าเกี่ยวข้อง

- ❖ ความยินยอมต้องอยู่แยกส่วนกับกับเงื่อนไขในการให้บริการ การขอความยินยอมจะต้องไม่สร้างว่าเป็นส่วนหนึ่งของสัญญาหรือเงื่อนไขในการให้บริการ หรือทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ โดยเฉพาะในกรณีที่มีการประมวลผลข้อมูลนั้นไม่จำเป็นสำหรับการให้บริการตามสัญญานั้นๆ ซึ่งหากการประมวลผลข้อมูลนั้นจำเป็นสำหรับการให้บริการให้ไปใช้ฐานสัญญา
- ❖ เนื้อหาของการขอความยินยอม การขอความยินยอมอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้
 - ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล (ชื่อ ที่อยู่ DPO ฯลฯ)
 - วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง
 - ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้
 - วิธีการประมวลผลข้อมูล
 - การใช้ระบบตัดสินใจอัตโนมัติ หรือ โปรไฟล์ (profiling) (หากมี)
 - การโอนข้อมูลไปต่างประเทศ
 - การเปิดเผยข้อมูลต่อบุคคลอื่น
 - ระยะเวลาในการจัดเก็บข้อมูล
 - วิธีการถอนความยินยอม
 - สิทธิต่างๆ ของเจ้าของข้อมูล โดยเฉพาะสิทธิในการถอนความยินยอม



แบบมาตรฐานใดที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่มากกว่าหนึ่งฐานประมวลผล หน่วยงานที่ออกแบบแบบมาตรฐานดังกล่าวต้องแสดงให้เห็นชัดเจนถึงส่วนของข้อมูลที่เก็บรวบรวมบนฐานความยินยอม เมื่อเป็นไปได้ให้กำหนดแยกออกมาต่างหาก (เป็นอีกหน้ากระดาษหนึ่งหรือชุดหนึ่งเอกสารหนึ่ง) และต้องได้รับการอนุมัติจากคณะกรรมการก่อนการประกาศใช้ใน ดย.

- ❖ วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง วัตถุประสงค์ในการประมวลผลข้อมูลแต่ละอย่างต้องชัดเจนและเฉพาะเจาะจง ผู้ควบคุมข้อมูลไม่สามารถเดิมวัตถุประสงค์ใหม่เองได้โดยไม่ขอความยินยอมใหม่ การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง

กรณีที่แบบมาตรฐานที่ใช้ในการเก็บรวบรวมข้อมูลส่วนบุคคลฐานความยินยอมเป็นไปมากกว่าหนึ่งวัตถุประสงค์ ให้หน่วยงานที่ออกแบบแบบมาตรฐานดังกล่าวจัดทำแบบมาตรฐานให้ง่ายต่อการเลือกความยินยอมต่อวัตถุประสงค์นั้น ๆ เมื่อเป็นไปได้ให้แยกออกมาต่างหาก กล่าวคือ หนึ่งหน้ากระดาษหรือหนึ่งชุดเอกสาร ต่อหนึ่งวัตถุประสงค์

- ❖ ความยินยอมต้องชัดเจนไม่คลุมเครือ การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็นการเลือกของเจ้าของข้อมูลเสมอ ดังนั้นเพื่อให้เจ้าของข้อมูลสามารถ "เลือก" ได้อย่างแท้จริงจึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเขียนเฉยหรือการเช็คลูกในช่องไว้ก่อน (pre-ticked box) ไม่ถือเป็นความยินยอมที่ชัดเจน
- ❖ การขอความยินยอมแบบชัดแจ้ง (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว การประมวลผลข้อมูลที่อ่อนไหวใช้การทำตามสัญญาเป็นฐานไม่ได้ จึงต้องใช้ฐานความยินยอมหรือฐานภารกิจของหน่วยงานรัฐหรือฐานประโยชน์อันชอบธรรมเป็นหลัก ดย. ต้องขอความยินยอมเป็นข้อเขียน และอาจให้ลงลายมือชื่อกำกับไว้ด้วยเพื่อลดความเสี่ยง หากเป็นการขอความยินยอมด้วยช่องทางอิเล็กทรอนิกส์ อาจใช้วิธีอื่นๆเช่นส่งอีเมลล์ อัปโหลดเอกสารสแกนที่มีลายมือชื่อ หรือใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น
- ❖ การให้ความยินยอมปากเปล่าก็เป็นความยินยอมแบบชัดแจ้งได้ แต่อาจยากต่อการพิสูจน์ ในกรณีของโทรศัพท์อาจทำได้หากให้ข้อมูลเพียงพอ มีทางเลือก และเนื้อหาชัดเจน โดยขอให้ผู้ใช้บริการกดปุ่มยืนยันหรือให้ความยินยอมปากเปล่าอย่างชัดเจน และมีการอัดเสียงบันทึกไว้

แบบมาตรฐานของ ดย. กรณีเป็นการประมวลผลฐานความยินยอมต้องลงลายมือชื่อเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญ พฤติการณ์ใด ๆ ที่แตกต่างออกไปตามบริบทและข้อจำกัดต้องให้คณะกรรมการพิจารณาเห็นชอบเป็นราย ๆ ไป

แบบมาตรฐานที่เป็นระบบสารสนเทศหรือรูปแบบดิจิทัล ต้องพิจารณาการใช้งานลายมือชื่ออิเล็กทรอนิกส์ (e-signature) หรือวิธีการอื่นใดที่ปลอดภัยหรือดีกว่า โดยอ้างอิงพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ และประกาศใด ๆ ที่เกี่ยวข้อง วิธีการที่แตกต่างไปจากนี้ คณะกรรมการต้องเห็นชอบ



การขอความยินยอมทางโทรศัพท์ต้องมีการอัดเสียง โดยต้องมีการตรวจสอบความเป็นเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะบันทึกเสียง

- ❖ การเคลื่อนไหวทางกายภาพ (physical motion) เช่น การเลื่อนขาไปบนตำแหน่งที่กำหนดบนหน้าจอ (swipe bar) การโบกมือให้กล้อง การหมุนโทรศัพท์ตามเข็มนาฬิกา ฯลฯ อาจถือเป็นการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) ได้ แต่ต้องออกแบบให้ลำดับขั้นตอนการขอความยินยอม (consent flow) นั้นให้ข้อมูลชัดว่าพฤติกรรมแต่ละอย่างนั้นหมายถึงอะไร เป็นการให้ความยินยอมสำหรับวัตถุประสงค์ใด และผู้ควบคุมข้อมูลต้องเก็บข้อมูลได้ด้วยวิธีใดในการขอความยินยอม อีกทั้งควรระมัดระวังไม่ให้เกิดความเหนื่อยล้าจากการคลิกให้ความยินยอมมากเกินไป (click fatigue) ทำให้การให้ความยินยอมแต่ละครั้งไม่มีความหมายที่แท้จริง

ดย. ต้องหลีกเลี่ยงการออกแบบระบบสารสนเทศใด ๆ ที่อาจก่อให้เกิดความสับสนและการให้ความยินยอมที่ผิดวัตถุประสงค์และเจตนาของเจ้าของข้อมูลส่วนบุคคล

- ❖ ออกแบบทางเลือกให้สามารถปฏิเสธที่จะให้ความยินยอมได้ หรือมีโอกาสดอนความยินยอมได้โดยไม่ได้รับผลกระทบมากเกินไป ผู้ควบคุมข้อมูลต้องประเมินและแยกแยะให้ชัดเจนว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาให้บริการ และข้อมูลใดจำเป็นต้องขอความยินยอมเพื่อให้บริการเสริม ดังนั้นเมื่อเจ้าของข้อมูลปฏิเสธการให้ความยินยอม หรือดอนความยินยอมจะต้องไม่กระทบเนื้อหาการให้บริการหลักแม้จะมีประสิทธิภาพน้อยลง และไม่ทำให้เกิดผลเป็นการลงโทษที่ดอนความยินยอม อีกทั้งการดอนความยินยอมจะต้องจะกระทำได้ง่ายในระดับเดียวกันกับการให้ความยินยอม

การขอความยินยอมและการดอนความยินยอมต้องง่ายเสมอกัน กล่าวคือแบบมาตรฐานใด ๆ มีการขอความยินยอมด้วยรูปแบบใดแล้วนั้นต้องมีช่องทางการดอนความยินยอมในรูปแบบเดียวกันเป็นอย่างน้อย

การดอนความยินยอมต้องกระทบต่อการขอความยินยอมได้ (reconcile) กล่าวคือทุก ๆ คำร้องขอดอนความยินยอมต้องมีหลักฐานของการให้ความยินยอมที่ตรงกัน เจ้าหน้าที่ห้ามรับคำเสนอดอนความยินยอมโดยปราศจากหลักฐานของการให้ความยินยอมก่อนนั้น ในสถานการณ์ที่ต้องสืบค้นหลักฐานการให้ความยินยอมและใช้เวลานาน ให้เจ้าหน้าที่ยื่นเสนอรับคำร้องขอของเจ้าของข้อมูล เพื่อแจ้งผลให้ทราบในภายหลังภายใน ๓ วันทำการ

คำร้องขอดอนความยินยอมใด ๆ ที่ไม่มีการให้ความยินยอมไว้ก่อนนั้น เจ้าหน้าที่ต้องพิจารณาส่งเรื่องให้คณะทำงานสืบค้นจนประจักษ์ ก่อนการแจ้งผลแก่เจ้าของข้อมูลส่วนบุคคล

ข้อควรระวังในการใช้ฐานความยินยอม

ข้อควรระวังในการจัดการความยินยอม ผู้ควบคุมข้อมูลพึงระวังในการจัดการความยินยอมโดยเฉพาะประเด็น

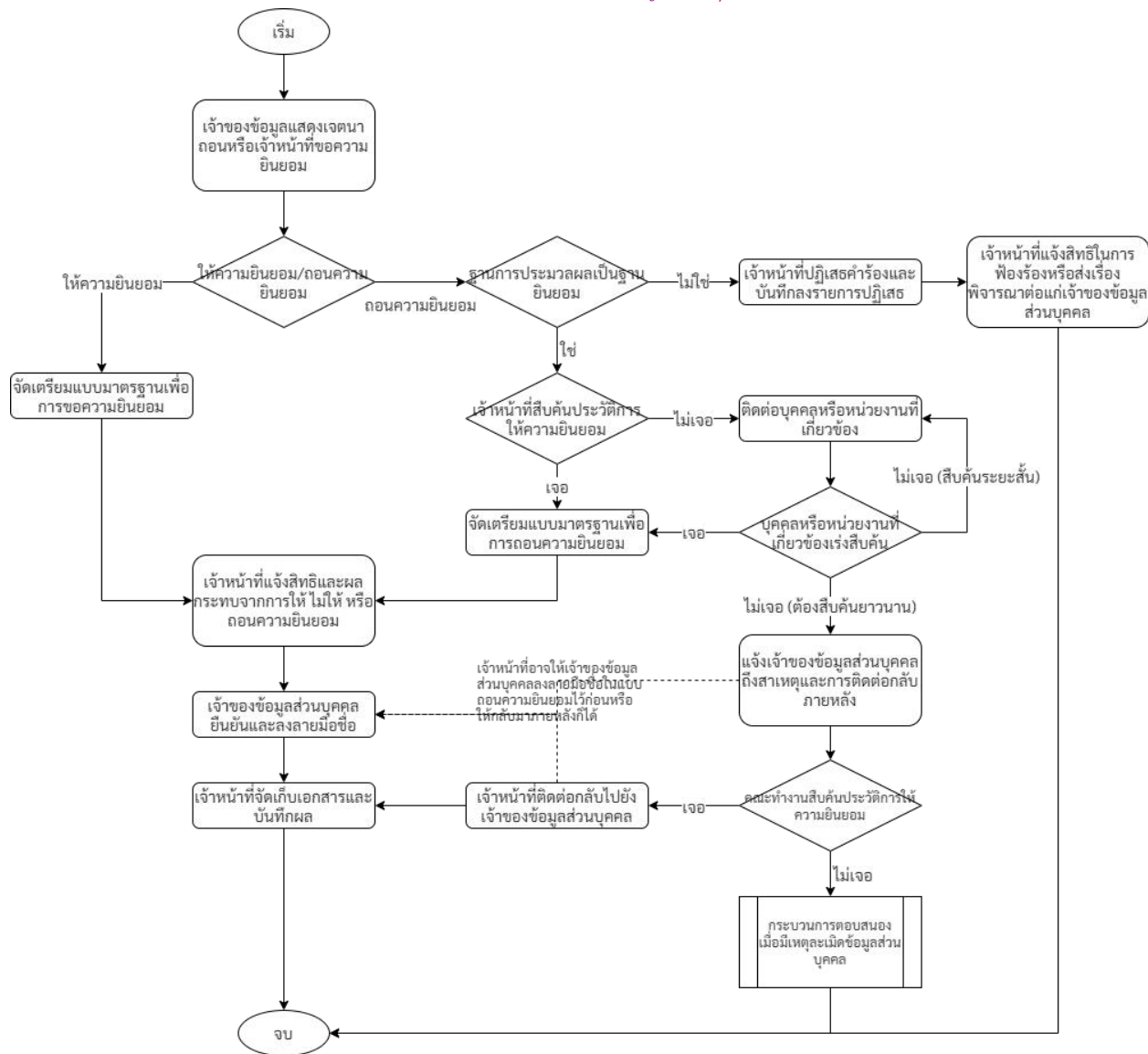
ดังต่อไปนี้

- ❖ ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น



- ❖ บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม
- ❖ แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้
- ❖ กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง
- ❖ กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม
- ❖ เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเจ้าของข้อมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว
- ❖ ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

กระบวนการขอและถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Consent Management Procedure)



ภาพที่ ๒ แผนผังกระบวนการขอและถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคล



กล่าวโดยสรุปสาระสำคัญของกระบวนการขอและถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ดังนี้

๑. เจ้าหน้าที่เตรียมแบบมาตรฐานในการขอและถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและมั่นใจว่ามีการแจ้งถึงสิทธิและผลกระทบจากการให้ความยินยอม ไม่ให้ความยินยอม และการถอนความยินยอม
๒. ในกรณีการถอนความยินยอม เจ้าหน้าที่ต้องสืบค้นจนมั่นใจว่าพบหลักฐานความยินยอมที่เจ้าของข้อมูลเคยให้ไว้ (เว้นแต่เป็นข้อมูลที่มีการเก็บไว้ก่อนหน้าที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้)
 - ๒.๑ กรณีสืบค้นไม่พบในระยะเวลาอันสั้น: เจ้าหน้าที่ควรพิจารณาช่องทางการรับเรื่องดังกล่าวไว้เพื่อการสืบค้นความยินยอมดังกล่าวต่อไป และดำเนินการติดต่อเจ้าของข้อมูลส่วนบุคคลในภายหลังเพื่อแจ้งให้รับทราบผลการถอนความยินยอมหรือปัญหาอุปสรรค กรณีดังกล่าวเจ้าหน้าที่อาจให้เจ้าของข้อมูลยื่นเรื่องการถอนไว้ก่อนหรือให้กลับมาในภายหลังก็ได้
 - ๒.๒ กรณีเกิดอุบัติเหตุละเมิดข้อมูลส่วนบุคคล: อันหมายถึงหลักฐานการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลดังกล่าวสูญหาย ให้คณะทำงานดำเนินการตามกระบวนการตอบสนองต่อเหตุละเมิดต่อไป
๓. แบบมาตรฐานต้องได้รับการลงลายมือชื่อเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญ เว้นแต่เป็นกรณีอื่น อาทิ ผู้เยาว์หรือผู้ไร้ความสามารถ เจ้าหน้าที่พิจารณาตามหลักกฎหมายหรือติดต่อคณะทำงานเพื่อขอข้อมูลประกอบการปฏิบัติภารกิจ และจัดเก็บเอกสารทั้งหมดไว้ตามระเบียบการคุ้มครองเอกสารของหน่วยงาน
๔. ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในฐานแห่งการประมวลผล ให้เจ้าหน้าที่อธิบายถึงความจำเป็นในการปฏิเสธรายการคำถอนความยินยอมตามหลักกฎหมาย พร้อมแจ้งถึงฐานแห่งการประมวลผลที่แท้จริงแก่เจ้าของข้อมูลส่วนบุคคล อนึ่งคำปฏิเสธการถอนความยินยอมต้องได้รับการบันทึกไว้เป็นลายลักษณ์อักษรและเก็บเป็นหลักฐานสำคัญต่อการบริหารจัดการและคุ้มครองข้อมูลส่วนบุคคล

ฐานประโยชน์สำคัญต่อชีวิต

กรณีที่มีการประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ดย. จะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสถานะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว

ในบริบทของ ดย. นั้น เนื่องจากข้อมูลส่วนบุคคลของประชาชน อาจจะมีได้เป็นประโยชน์ในฐานนี้เท่าไรนัก **ยกเว้นการเข้าช่วยเหลือเด็กและเยาวชนที่ถูกทารุณกรรมในระดับที่อันตรายถึงชีวิต** ในกรณีที่เกิดเหตุการณ์ใด ๆ ที่มีการกล่าวถึงการขอเข้าถึงหรือขอให้ ดย. เปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์สำคัญต่อชีวิต ดย. ต้องพิจารณาและตรวจสอบอย่างรัดกุม และตรวจสอบด้วยวิธีการที่รวดเร็วและสามารถใช้ประกอบการตัดสินใจได้ในระดับที่ไม่กระทบต่อเจ้าของข้อมูลส่วนบุคคลสูงเกินไป



ในกรณีที่มีการขอเข้าถึงหรือขอให้ ดย. เปิดเผยข้อมูลเจ้าหน้าที่พนักงาน ข้าราชการ ตลอดจนบุคลากรของ ดย. เพื่อประโยชน์สำคัญต่อชีวิต ให้หน่วยงานที่เกี่ยวข้องกับฝ่ายบุคคลหรือต้นสังกัดเจ้าหน้าที่คนนั้นพิจารณาอนุมัติและดำเนินการตรวจสอบแหล่งคำร้องขอเพื่อยืนยันในทันที

เมื่อพบว่าคำร้องดังกล่าวเป็นการฉ้อฉล หลอกลวง หรือขอเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ ให้เจ้าหน้าที่ที่เกี่ยวข้องเร่งดำเนินการตามกระบวนการปฏิบัติการด้านเหตุละเมิดข้อมูลส่วนบุคคล

ฐานสัญญา

กรณีที่การประมวลผลข้อมูลจำเป็นต้องการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่าง ดย. และเจ้าของข้อมูล หรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญา ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหว (sensitive data) ใช้การทำตามสัญญาเป็นฐานในการประมวลผลไม่ได้

การประมวลผลข้อมูลบนฐานสัญญานี้จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สาม จะกระทำได้โดยใช้ฐานความยินยอม หรือฐานผลประโยชน์อันชอบธรรม (ซึ่งจะต้องมีการประเมินแล้วว่าผลประโยชน์ที่เกิดแก่คู่สัญญาหรือบริษัทนั้นไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล (ในที่นี้คือคู่สมรส) โดยไม่เกินขอบเขตที่ตัวเจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผลด้วย) ไม่ใช่ฐานสัญญา

ในกรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับ ดย. โดยประมวลผลข้อมูลที่ทำเป็นต่อการปฏิบัติตามสัญญานั้นๆ ถือเป็น การประมวลผลตามฐานสัญญา ดังนั้นผู้ประมวลผลข้อมูลไม่จำเป็นต้องขอความยินยอมเพิ่มเติมแต่อย่างใด

การประมวลผลข้อมูลนั้นอาจเกิดขึ้นโดยใช้ฐานสัญญาที่มีมากกว่าหนึ่ง

ดย. เป็นหน่วยงานที่ใช้บริการสาธารณะตามอำนาจที่กฎหมายได้ให้ไว้ อนึ่งการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลภายใต้ ฐานการปฏิบัติตามสัญญานั้นย่อมเกิดขึ้นได้โดยยากด้วยบริบทขององค์กร เว้นแต่เสียว่ามีกรว่าจ้างงานเป็นครั้งคราวไป โดยเป็นสภาพการจ้างแรงงานที่ความสัมพันธ์ของบุคคลดังกล่าวกับ ดย. เป็นไปตามข้อตกลงในสัญญาตามประมวลกฎหมายแพ่ง และพาณิชย์ ซึ่งการประมวลผลข้อมูลส่วนบุคคลย่อมเป็นไปตามเงื่อนไขและบทบาทหน้าที่ที่กำหนดไว้ตามสัญญา

ข้อควรระวังในการใช้ฐานการปฏิบัติตามสัญญา

- ❖ ในกรณีที่สามารถปฏิบัติหน้าที่ตามสัญญาหรือตามคำขอได้โดยไม่ต้องประมวลผลข้อมูลส่วนบุคคลถือว่าเป็น "ไม่จำเป็น" ดังนั้น ดย. ควรประเมินขอบเขตของสัญญาให้แน่ชัด เพื่อจะได้ทราบถึงขอบเขตของข้อมูลที่เกี่ยวข้องในการปฏิบัติตามสัญญา อีกทั้ง การประมวลผลข้อมูลเพื่อปฏิบัติตามสัญญาจะต้องเป็นไปอย่างเฉพาะเจาะจงตามที่ระบุในสัญญานั้นๆ
- ❖ ความจำเป็น ในที่นี้จำกัดอยู่แค่เพียงการปฏิบัติตามสัญญาตามปกติของการดำเนินงานให้เป็นไปตามสัญญาเท่านั้น ไม่รวมถึงกรณีที่เกิดปัญหาหรือข้อพิพาทที่เกี่ยวข้อง



ฐานกิจสาธารณะ/อำนาจรัฐ

กรณีที่มีการประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงานศาลยุติธรรม สำนักงานเลขาธิการสภาผู้แทนราษฎรและวุฒิสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่ในการใช้อำนาจที่รัฐได้มอบหมายให้เพื่อผลประโยชน์สาธารณะตามกฎหมาย เช่น การให้บริการสอบใบอนุญาตขับขี่รถยนต์ โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

ฐานนี้ใช้ไม่ได้ในกรณีที่สามารถดำเนินงานตามภารกิจของรัฐได้โดยไม่จำเป็นต้องประมวลผลข้อมูลส่วนบุคคล เช่น ธนาคารแห่งประเทศไทยสามารถตรวจสอบข้อมูลหนี้ครัวเรือนโดยทั่วไปได้โดยไม่ต้องประมวลผลข้อมูลส่วนที่สามารถระบุตัวตน แต่อาศัยเฉพาะการประมวลผลข้อมูลสถิติที่ธนาคารพาณิชย์ส่งให้ก็เพียงพอ

การประมวลผลบนฐานภารกิจของรัฐไม่ได้ให้อำนาจโดยไร้เงื่อนไข หลักการความได้สัดส่วนยังเป็นเงื่อนไขสำคัญ และมีหน้าที่ของผู้ควบคุมข้อมูลที่ต้องปฏิบัติตามอยู่เช่นเดียวกับฐานอื่นๆ โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ และโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล อนึ่ง ในกรณีที่เป็นการประมวลผลโดยหน่วยงานของรัฐ จำเป็นต้องพิจารณาหลักความจำเป็นในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐ มาตรา ๒๓(๑) ประกอบ อีกทั้งต้องสอดคล้องกับหลักการของรัฐธรรมนูญมาตรา ๗๗ เรื่องหลักความจำเป็นในการใช้เครื่องมือทางกฎหมายและการใช้อำนาจรัฐ รวมถึงการประเมินผลกระทบของการออกกฎหมาย (Regulatory Impact Assessment - RA) ควรคำนึงถึงผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วย

แม้มาตรา ๔ ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล จะยกเว้นการบังคับใช้กับกิจกรรมของรัฐบางประการ แต่ก็ยังกำหนดให้การมีการจัดการรักษาความมั่นคงปลอดภัยตามมาตรฐานตามวรรค ๓ ของมาตราเดียวกันด้วย และไม่ได้ยกเว้นหน้าที่ของทั้งองค์กร ซึ่งในความเป็นจริงแล้ว กิจกรรมของภาครัฐส่วนใหญ่นั้นสามารถใช้ฐานภารกิจของรัฐในการประมวลผลได้อยู่แล้ว หากการประมวลผลข้อมูลเกิดขึ้นโดยปฏิบัติตามมาตรฐานของการใช้ฐานภารกิจของรัฐก็จะลดความเสี่ยงของผู้ควบคุมข้อมูลลง

ดย. เป็นหน่วยงานของรัฐที่ไม่ตกในข้อยกเว้นตามมาตรฐาน ๔ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล อีกประการหนึ่ง การปฏิบัติหน้าที่ของ ดย. บางภารกิจอาจมีการเก็บ รวบรวมใช้ เผยข้อมูลส่วนบุคคล

หน่วยงานใด ที่มีภารกิจหรือโครงการภายใต้ภารกิจที่ได้รับอำนาจตามกฎหมาย ย่อมพิจารณาถึงการประมวลผลข้อมูลส่วนบุคคลและความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล เมื่อปรากฏว่ามีโครงการหรือกิจกรรมใด ๆ ที่เกิดขึ้นใหม่ภายใต้ภารกิจพันธกิจของหน่วยงานที่ต้องมีการประมวลผลข้อมูลส่วนบุคคลนั้น ให้หน่วยงานต้นสังกัดทำการวิเคราะห์และจัดแสดงถึงรายการข้อมูลส่วนบุคคลพร้อมวัตถุประสงค์แห่งการประมวลผลชี้แจงแก่คณะทำงาน เมื่อคณะทำงานพิจารณาแล้วว่าไม่มีความเสี่ยงหรือผลกระทบสูงก็ย่อมดำเนินการได้ตามกรอบแนวทางและนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของ ดย.

กรณีที่คณะทำงานวิเคราะห์และพบว่าการประมวลผลข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูง ให้ดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (PIA: Privacy Impact Assessment) อย่างละเอียดแล้วนำเสนอต่อคณะกรรมการเพื่อพิจารณาอนุมัติ ในระหว่างพิจารณาของคณะกรรมการ ให้หน่วยงานต้นสังกัดละเว้นหรืองดเว้นการประมวลผลข้อมูลส่วนบุคคล



บุคคลจนกว่าจะมีมติอนุมัติ หรือดำเนินการประมวลผลข้อมูลส่วนบุคคลเฉพาะขอบเขตที่ไม่มีผลกระทบสูงหรือตามคำแนะนำของคณะกรรมการท่านนั้น

ฐานประโยชน์อันชอบด้วยกฎหมาย

ดย. อาจประมวลผลข้อมูลส่วนบุคคลในกรณีที่เป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของ ดย. หรือบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การบริหารงานของรัฐ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ การปฏิบัติตามกฎหมายของต่างประเทศที่จำเป็น เป็นต้น

การใช้ฐานประโยชน์อันชอบธรรม (legitimate interest) ในการประมวลผลข้อมูลทำให้มีขอบเขตค่อนข้างกว้างและค่อนข้างยืดหยุ่นในการปรับใช้ ดังนั้น ดย. จะต้องใช้ดุลยพินิจอย่างมาก เพื่อชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมนั้นไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล โดยผู้ประมวลผลข้อมูล ดย. จะต้องระบุได้ว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับ และอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังต้องมีหน้าที่ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สอดคล้องกับประโยชน์อันชอบธรรมที่จะได้รับด้วย การใช้ดุลยพินิจเช่นนี้ย่อมทำให้เกิดความเสี่ยงมากในการตัดสินใจผิดพลาดซึ่ง ดย. อาจต้องรับผิดชอบภายหลังได้

ดย. ไม่อาจอ้างได้ว่าเจ้าของข้อมูลควรจะคาดหมายการประมวลผลข้อมูลได้ เพราะประกาศไว้ในนโยบายความเป็นส่วนตัวตัวไว้แล้ว หากเนื้อหานั้นไม่ได้เฉพาะเจาะจงและสามารถมั่นใจได้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีโอกาสได้อ่านจริงๆ เว้นแต่เสียว่ามีแบบมาตรฐานที่ให้การลงลายมือยืนยันถึงการได้อ่านข้อตกลง เช่น

ในการอ้างฐานนี้เพื่อประมวลผล ดย. ต้องแน่ใจว่ามีความจำเป็นในการประมวลผลจริง ผลประโยชน์อันชอบธรรมนั้นมีความชัดเจน และต้องชั่งน้ำหนักระหว่างผลประโยชน์กับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ฐานปฏิบัติหน้าที่ตามกฎหมาย

กรณีการประมวลผลข้อมูลจำเป็นต่อการปฏิบัติหน้าที่ที่ผู้ควบคุมข้อมูลนั้นมีตามที่กฎหมายกำหนด ผู้ควบคุมข้อมูล (ซึ่งมักเป็นองค์กรเอกชน) จะต้องระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ

ฐานนี้จะใช้ไม่ได้หากผู้ควบคุมข้อมูลสามารถใช้ดุลยพินิจได้ว่าจะประมวลผลข้อมูลนี้เพื่อทำตามกฎหมาย หรือมีทางเลือกอื่นที่เหมาะสมในการปฏิบัติตามกฎหมายนอกเหนือจากการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล

ฐานจดหมายเหตุ/วิจัย/สถิติ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดฐานในการประมวลผลข้อมูลหนึ่งที่แตกต่างไปจากกฎหมายของประเทศอื่นรวมถึง GDPR คือการจัดทำเอกสารประวัติศาสตร์จดหมายเหตุ และการศึกษาวิจัยและสถิติ



ความหมายของการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสภิตินั้นอาจกินความได้กว้างขวาง เนื่องจากการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัยและสภิตินั้นโดยทั่วไปถูกมองว่าเป็นเพียง "วิธีการ" เพื่อให้บรรลุวัตถุประสงค์อย่างใดอย่างหนึ่งก็ได้ ซึ่งแตกต่างจากการประมวลผลในฐานอื่นๆ ที่เน้นไปที่ลักษณะของวัตถุประสงค์เป็นหลัก ซึ่งแต่ละฐานก็อ้างอิงความชอบธรรมในการประมวลผลในรูปแบบต่างๆ ทั้งจากกฎหมาย (ฐานภารกิจของรัฐ ฐานการปฏิบัติตามกฎหมาย) จากการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลเอง (ฐานความยินยอม) จากผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล(ฐานประโยชน์อันสำคัญต่อชีวิต และจากผลประโยชน์ของผู้ควบคุมข้อมูลหรือบุคคลที่สามที่เหนือกว่าเจ้าของข้อมูลส่วนบุคคล (ฐานผลประโยชน์อันชอบธรรม) ดังนั้นใน GDPR จึงกำหนดให้การศึกษาวิจัยและสภิติจจะต้องอ้างอิงฐานใดฐานหนึ่งใน ๖ ฐานประกอบด้วยเสมอ

ในทางปฏิบัติจึงเป็นไปได้ที่ผู้ควบคุมข้อมูลจะอ้างอิงแต่ฐานนี้เพียงฐานเดียว และจะทำให้ไม่สอดคล้องกับทางปฏิบัติสากล รวมถึง GDPR ด้วย ทำให้มีความเสี่ยงเมื่อดำเนินการกับข้อมูลของคน โดยเฉพาะกรณีของคนในสหภาพยุโรปและเมื่อต้องทำธุรกรรมกับประเทศในสหภาพยุโรป

การประมวลผลบนฐานนี้มีเงื่อนไขสำคัญคือต้องจัดให้มีมาตรการปกป้องที่เหมาะสม โดยอย่างน้อยต้องเป็นไปตามที่คณะกรรมการประกาศกำหนด ซึ่งหากผู้ควบคุมข้อมูลจัดให้มีมาตรการที่สอดคล้องกับมาตรฐานจริยธรรมของระเบียบวิธีในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัยและสภิติของการศึกษาประเภทต่างๆ ด้วย ก็จะทำให้การส่งต่อข้อมูลหรือนำไปใช้งานต่อในบริบทอื่นๆ ก็จะเป็นไปได้ง่ายและถูกต้องตามเงื่อนไขของกฎหมายของประเทศอื่นๆ ด้วยอีกทั้งยังคาดหมายได้ว่าประกาศของคณะกรรมการก็น่าจะต้องอ้างอิงไปตามมาตรฐานสากลของระเบียบวิธีเหล่านี้ด้วย

มาตรการปกป้องที่เหมาะสมสามารถอ้างอิงตามตามมาตรฐานจริยธรรมของสาขาวิชาต่างๆ ที่เกี่ยวข้องกับการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสภิติ ซึ่ง ถือปฏิบัติตามแนวทางที่เป็นสากลอยู่แล้ว และสอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล คือ หลักความจำเป็น หลักความได้สัดส่วน และการเคารพสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นต่อการบรรลุวัตถุประสงค์ของการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสภิตินั้นย่อมไม่สามารถอ้างอิงฐานนี้ได้