ประกาศสำนักงานสลากกินแบ่งรัฐบาล
เรื่อง นโยบายข้อมูล (Data Policies)

ด้วยสำนักงานสลากกินแบ่งรัฐบาล ตระหนักถึงความสำคัญของการกำกับดูแลธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารจัดการข้อมูลขององค์กรมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดต่างๆ ซึ่งนำไปสู่ความเป็นองค์กรที่มีประสิทธิภาพในการดำเนินงานและการบริหารจัดการที่ดี โปร่งใส เป็นธรรม และตรวจสอบได้ จึงได้กำหนดนโยบายข้อมูล เพื่อให้ผู้บริหารและพนักงานยึดถือเป็นแนวทางปฏิบัติดังนี้

๑. หมวดทั่วไป (General Domain)

๑.๑ โครงสร้างการกำกับดูแลธรรมาภิบาลข้อมูล ประกอบด้วย

๑.๑.๑ คณะกรรมการนโยบายและกำกับดูแลธรรมาภิบาลข้อมูล ประกอบด้วย ผู้อำนวยการเป็นประธานคณะกรรมการ และผู้บริหารระดับสูงเป็นคณะกรรมการ โดยให้คณะกรรมการมีความรับผิดชอบและบทบาทหน้าที่ ดังนี้

(๑) กำหนดนโยบายธรรมาภิบาลข้อมูล เกณฑ์การวัดคุณภาพ ระเบียบและข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญของข้อมูลในการกำกับดูแลข้อมูล

(๒) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการกำกับดูแลข้อมูล

(๓) สื่อสารถึงความสำคัญ ขอบเขต นโยบาย และเป้าประสงค์ของการกำกับดูแลข้อมูล

(๔) ดำเนินการกำกับดูแลข้อมูลให้มีคุณภาพและเกิดประโยชน์สูงสุดต่อสำนักงานฯ

(๕) ทบทวนและพิจารณาปรับปรุงแก้ไขแนวปฏิบัติและมาตรฐานของการกำกับดูแลข้อมูล

(๖) เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

(๗) สนับสนุน ส่งเสริม และพิจารณาจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงาน

(๘) ส่งเสริมและสนับสนุนการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างหน่วยงาน

๑.๑.๒ คณะทำงานบริกรข้อมูลเพื่อจัดทำธรรมาภิบาลข้อมูล ประกอบด้วย รองผู้อำนวยการหรือผู้ช่วยผู้อำนวยการที่กำกับดูแลสำนักเทคโนโลยีสารสนเทศ เป็นประธานคณะทำงาน และพนักงานที่ได้รับการแต่งตั้งเป็นคณะทำงาน โดยให้คณะทำงานมีความรับผิดชอบและบทบาทหน้าที่ ดังนี้

(๑) นิยาม กำหนดความหมายของคำอธิบายข้อมูล (Meta-Data)

(๒) กำหนดความต้องการด้านคุณภาพและความมั่นคงปลอดภัยสารสนเทศ

(๓) นำเสนอร่างนโยบายรวมถึงกระบวนการที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลต่อคณะกรรมการนโยบายและกำกับดูแลธรรมาภิบาลข้อมูล

(๔) ดูแลรักษาข้อมูลบนระบบสารสนเทศของสำนักงานฯ รวมถึงข้อมูลที่มีการเชื่อมโยงระหว่างหน่วยงาน ให้มีความมั่นคงปลอดภัย

/๒...

(๕) ตรวจสอบคุณภาพข้อมูล และจัดทำรายงานผลวิเคราะห์ผลจากการตรวจสอบ

(๖) รายงานผลการดำเนินงานต่อคณะกรรมการนโยบายและกำกับดูแลธรรมาภิบาลข้อมูล และผู้ที่เกี่ยวข้องอื่นๆ

๑.๑.๓ คณะทำงานบริหารจัดการข้อมูลส่วนบุคคล (PDPA Working Team) ประกอบด้วยตัวแทนจากหน่วยงานภายในสำนักงานฯ ที่มีการเข้าถึงและใช้งานข้อมูลส่วนบุคคล โดยให้คณะทำงานมีความรับผิดชอบและบทบาทหน้าที่ ดังนี้

(๑) จัดทำบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล (RoPA)

(๒) ประเมินและบริหารความเสี่ยงในประเด็นที่เกี่ยวข้องกับการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

(๓) ประเมินผลกระทบต่อข้อมูลส่วนบุคคล (DPIA) และกำหนดมาตรการเพื่อลดผลกระทบหรือลดโอกาสในการละเมิดข้อมูลส่วนบุคคล

(๔) กำหนดและทบทวนปรับปรุงขั้นตอนการรับมือเมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคล

(๕) ออกแบบและปรับปรุงกระบวนทำงานที่เกี่ยวกับการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปปฏิบัติตามแนวปฏิบัติในการบริหารจัดการข้อมูลของสำนักงานฯ

(๖) ควบคุมการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามตามสัญญาหรือข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล

(๗) ประสานงาน ให้ความร่วมมือ และให้ข้อมูลกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เมื่อมีการตรวจสอบการดำเนินงาน หรือเมื่อมีคำร้องขอ/ข้อร้องเรียนของเจ้าของข้อมูลส่วนบุคคล หรือมีการสอบสวนเมื่อเกิดปัญหาเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๘) พัฒนาทักษะความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง

๑.๑.๔ หน่วยงานเจ้าของข้อมูล ได้แก่ งาน/กลุ่มงาน กอง สำนัก ที่คณะกรรมการนโยบายและกำกับดูแลธรรมาภิบาลข้อมูลกำหนดให้เป็นหน่วยงานเจ้าของข้อมูล โดยให้หน่วยงานเจ้าของข้อมูลมีความรับผิดชอบและบทบาทหน้าที่ ดังนี้

(๑) ปฏิบัติตามนโยบายข้อมูล รวมถึงมาตรการต่างๆ ที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล

(๒) กำหนดลำดับชั้นความลับ และกำหนดสิทธิ์ในการเข้าถึงข้อมูล

(๓) สนับสนุนการดำเนินงานของคณะทำงานบริกรข้อมูลเพื่อจัดทำธรรมาภิบาลข้อมูล

๑.๑.๕ ผู้ใช้ข้อมูล ได้แก่ ผู้บริหาร/พนักงาน/ลูกจ้าง ที่นำข้อมูลไปใช้ในการทำงาน ซึ่งได้รับสิทธิ์จากหน่วยงานเจ้าของข้อมูลให้เข้าถึง ประมวลผลและนำข้อมูลไปใช้ โดยให้ผู้ใช้ข้อมูลมีความรับผิดชอบและบทบาทหน้าที่ ดังนี้

(๑) ปฏิบัติตามนโยบายข้อมูล รวมถึงมาตรการต่างๆ ที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล

(๒) นำข้อมูลไปใช้ตามสิทธิที่ได้รับจากหน่วยงานเจ้าของข้อมูล

(๓) ไม่นำข้อมูลไปใช้เพื่อประโยชน์ส่วนตัว

/๓...

๑.๒ ขอบเขตของข้อมูล ได้แก่

๑.๒.๑ ข้อมูลที่อยู่ในรูปแบบเอกสาร ได้แก่ สัญญา ข้อตกลง ประกาศ คำสั่ง แบบฟอร์ม รายงาน บันทึกข้อความ เอกสารประกอบ หรือเอกสารรูปแบบอื่นใดที่ใช้ในการดำเนินงานของสำนักงานฯ ทั้งที่เป็นเอกสารต้นฉบับและสำเนา

๑.๒.๒ ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ หรือแบบดิจิทัล ได้แก่ เสียง ภาพ ภาพเคลื่อนไหว ฐานข้อมูล ไฟล์ทุกชนิด ที่ใช้ในการดำเนินงานต่างๆ ของสำนักงานฯ รวมถึงมีการจัดเก็บและเผยแพร่โดยสำนักงานฯ

๑.๓ การรักษาคุณภาพและความมั่นคงปลอดภัยของข้อมูล

๑.๓.๑ ข้อมูลของสำนักงานฯ ต้องมีการบริหารจัดการเพื่อให้ข้อมูลมีคุณภาพและมีความมั่นคงปลอดภัย โดยมีการจัดทำนิยามและกำหนดความหมายของคำอธิบายข้อมูล (Meta-Data) มีการจัดลำดับชั้นความลับ มีการกำหนดสิทธิ์ในการเข้าถึง มีการจัดเก็บที่เหมาะสมเพื่อป้องกันการสูญหาย ถูกทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๑.๓.๒ มีการตรวจประเมินคุณภาพข้อมูล และประเมินความมั่นคงปลอดภัยของข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๑.๓.๓ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งข้อมูลที่สำคัญของสำนักงานฯ และข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยเป็นไปตามกฎหมายที่เกี่ยวข้อง

๑.๓.๔ จัดให้มีแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (Data Breach) โดยเป็นไปตามกฎหมายที่เกี่ยวข้อง

๑.๔ การตรวจสอบและทบทวนนโยบาย

๑.๔.๑ มีการตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินงานของสำนักงานฯ อย่างน้อยปีละ ๑ ครั้ง

๑.๔.๒ มีการทบทวนนโยบายข้อมูลอย่างน้อยปีละ ๑ ครั้ง และดำเนินการปรับปรุงอย่างต่อเนื่อง

๑.๕ การสื่อสารและเผยแพร่นโยบาย

๑.๕.๑ มีการประกาศนโยบายตามช่องทางการสื่อสารที่เป็นทางการของสำนักงานฯ

๑.๕.๒ มีการฝึกอบรมให้กับผู้บริหารและพนักงาน เพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐ และการบริหารจัดการข้อมูล

๒. หมวดการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Domain)

๒.๑ มีการกำหนดแนวปฏิบัติในการจัดเก็บและทำลายข้อมูล

๒.๒ มีการกำหนดกระบวนการในการจัดเก็บและทำลายข้อมูลที่ชัดเจน

๒.๓ มีการกำหนดความหมายของคำอธิบายข้อมูล (Meta-Data) ที่จัดเก็บ

๒.๔ มีการกำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

/๔...

๒.๕ มีการกำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล

๒.๖ มีการกำหนดสิทธิ์การเข้าถึงข้อมูลและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

๒.๗ มีการจัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ ไม่ซ้ำซ้อน และเป็นปัจจุบันอยู่เสมอ

๒.๘ ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมหรือหน่วยงานเจ้าของข้อมูลต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุม หรือไม่ขัดต่อข้อกฎหมายใดๆ

๒.๙ มีการกำหนดระยะเวลาในการทำลายข้อมูลที่ไม่ได้ใช้งาน และควรเก็บคำอธิบายข้อมูล (Meta-Data) ไว้ตรวจสอบภายหลัง

๒.๑๐ มีการสร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้อง

๒.๑๑ มีระบบหรือกระบวนการสำหรับตรวจสอบเพื่อลบทำลายข้อมูลส่วนบุคคลตามสิทธิในการขอลบข้อมูลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่ไม่ขัดต่อข้อกฎหมายใดๆ

๓. หมวดการประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use Domain)

๓.๑ มีการกำหนดแนวปฏิบัติเรื่องการควบคุมการประมวลผลข้อมูลและการใช้ข้อมูล

๓.๒ มีการกำหนดกระบวนการในการประมวลผลและการใช้ข้อมูล ตั้งแต่ขั้นตอนเตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๓.๓ มีการกำหนดวัตถุประสงค์ในการประมวลผล และการนำข้อมูลไปใช้

๓.๔ กรณีที่เป็นข้อมูลส่วนบุคคลให้เป็นไปตาม ขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

๓.๕ มีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๓.๖ มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัย และการเลือกผู้ประมวลผลภายนอกที่มีการจัดการระบบรักษาความปลอดภัยที่เหมาะสม

๓.๗ มีข้อตกลงกับผู้ประมวลผลข้อมูล เพื่อควบคุมให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

๓.๘ กรณีที่มีการโอนข้อมูลไปยังต่างประเทศ ต้องทำให้ถูกต้องตามกฎหมาย

๓.๙ มีการสร้างความรู้ความเข้าใจในการประมวลผลและการใช้ข้อมูลแก่ผู้ที่เกี่ยวข้อง

๔. หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล (Data Exchange and Integration Domain)

๔.๑ มีการพิจารณาตามแนวทางการคัดเลือกคู่ความร่วมมือตามที่สำนักงานฯ กำหนด

๔.๒ มีการกำหนดแผนงานโครงการที่มีการแลกเปลี่ยนและการเชื่อมโยงข้อมูลไว้ในแผนดำเนินงานประจำปีของสำนักงานฯ

๔.๓ มีการกำหนดแนวปฏิบัติเรื่องการควบคุมคุณภาพข้อมูลและการจัดการด้านความมั่นคงปลอดภัยข้อมูล

๔.๔ มีการกำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลที่ชัดเจน ตั้งแต่ขั้นตอนเตรียมการเริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

/๕...

๔.๕ มีการกำหนดความหมายของคำอธิบายข้อมูล (Meta-Data) ที่ต้องเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

๔.๖ มีการทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูล และการนำข้อมูลไปใช้เพื่อควบคุมให้บุคคลหรือนิติบุคคลที่แลกเปลี่ยนข้อมูลดำเนินการให้เป็นไปตามกฎหมาย

๔.๗ มีการกำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๔.๘ มีการบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๔.๙ มีการตรวจสอบการเชื่อมโยงและแลกเปลี่ยนข้อมูล เพื่อให้มั่นใจว่าได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามสัญญาอนุญาตหรือข้อตกลง แนวปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยนและมาตรฐานตามที่กำหนด

๔.๑๐ มีมาตรการป้องกันมิให้บุคคลที่ได้รับข้อมูลส่วนบุคคลที่มิใช่ผู้ควบคุมข้อมูลอื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

๕. หมวดการเปิดเผยข้อมูล (Data Disclosure Domain)

ข้อมูลเปิด (Open Data) คือ “ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาตหรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด” ข้อมูลจากหน่วยงานภาครัฐที่สามารถเปิดเผยได้ จะอยู่ในรูปแบบที่เป็นมาตรฐานเปิด (Open Format) และไม่ใช่รูปแบบมาตรฐานเฉพาะ (Non-proprietary Format) ที่คนและเครื่องคอมพิวเตอร์สามารถอ่านและนำไปใช้ต่อยอดในการพัฒนาบริการในรูปแบบต่างๆ ได้ ข้อมูลเปิดถูกใช้เป็นเครื่องมือในการตรวจสอบความโปร่งใสในการดำเนินการของภาครัฐและความสามารถในการพัฒนาประเทศ ซึ่งสามารถวัดอันดับการเปิดเผยข้อมูลภาครัฐได้จากมาตรฐานตัวชี้วัด เช่น Open Data Index และ Open Data Barometer เพื่อให้อันดับการเปิดเผยข้อมูลภาครัฐสูงขึ้น ซึ่งแนวนโยบายในการเปิดเผยข้อมูล มีดังนี้

๕.๑ ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๕.๒ ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

๕.๓ ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

๕.๔ ควรมีการเปิดเผยคำอธิบายข้อมูล (Meta-Data) ควบคู่ไปกับข้อมูลที่เปิดเผย

๕.๕ มีการตรวจสอบว่าการเปิดเผยข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๕

พันโท

(หนุน ศันสนาคม)

ผู้อำนวยการสำนักงานสลากกินแบ่งรัฐบาล