

**(ร่าง) แนวปฏิบัติสำหรับการดำเนินการของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**

**(Data Protection Officer)**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 เพื่อให้เป็นไปตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (พระราชบัญญัติ)
และตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล กรมควบคุมโรคจึงได้กำหนดแนวทางสำหรับ การดำเนินการของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ดังนี้

1. **การแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**
	1. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรมีคุณสมบัติต่อไปนี้
		1. มีความเชี่ยวชาญในระดับที่เหมาะสม : ความเชี่ยวชาญในระดับที่เหมาะสมกับ
		ความละเอียดอ่อน จำนวน และความซับซ้อนของข้อมูลที่ได้รับการประมวลผล และการโอนข้อมูลส่วนบุคคลแบบเป็นระบบหรือการโอนข้อมูลส่วนบุคคลเป็นบางครั้ง
		2. มีความเข้าใจพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในเชิงลึก : เข้าใจพระราชบัญญัติอย่างแตกฉานและคอยติดตามเกี่ยวกับการพัฒนา การเปลี่ยนแปลง และการตีความพระราชบัญญัติ รวมถึงกฎหมายลำดับรอง แนวทางปฏิบัติ คำสั่ง คำตัดสิน และกฎหมายที่เกี่ยวข้องอื่นๆ
		ที่ออกโดยหน่วยงานและศาลที่มีอำนาจ
		3. มีความรู้เกี่ยวกับการดำเนินงานของกรมควบคุมโรคเพียงพอ
		4. มีความเข้าใจที่เพียงพอเกี่ยวกับกระบวนการประมวลผลข้อมูลส่วนบุคคล
		การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และระบบข้อมูลของกรมควบคุมโรค
	2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของกรมควบคุมโรค หรือบุคคล
	ที่สามที่ได้รับการว่าจ้างมาให้ปฏิบัติหน้าที่ตามสัญญาให้บริการ (มาตรา 41 วรรค 7) (โดยที่จะต้องเป็นไปตามข้อกำหนดอื่นๆ สำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เช่น จะต้องไม่มีความขัดกันของผลประโยชน์)
	3. ประเด็นหนึ่งที่ต้องพิจารณาตัดสินใจคือจะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
	จากภายในหรือภายนอก แม้ว่าจะสามารถมอบหมายหน้าที่นี้ให้แก่ผู้ให้บริการจากภายนอก แต่การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากภายนอกอาจทำให้เกิดปัญหาบางประการ เช่น

ก) ในบางกรณี การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากภายนอก อาจช่วยลดภาระการบริหารจัดการภายในที่เกี่ยวข้องกับตำแหน่งนี้

ข) อย่างไรก็ตาม เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับความช่วยเหลือ
อย่างเหมาะสมจากบุคลากรผู้เชี่ยวชาญทางเทคนิค (เช่น ฝ่ายเทคโนโลยีสารสนเทศ ผู้บริหารจัดการระบบ)
โดยผู้ให้บริการจากภายนอกอาจไม่มีความคุ้นชินเท่าที่ควรกับระบบภายใน สิ่งอำนวยความสะดวก และการติดต่อต่าง ๆ ที่จำเป็นต่อหน้าที่นี้ ในทางตรงกันข้าม ผู้บริหารหรือพนักงานภายใน จะสามารถเข้าถึงและคุ้นเคย
กับระบบภายใน สิ่งอำนวยความสะดวก และการติดต่อต่าง ๆ ทำให้สามารถให้ความช่วยเหลือสนับสนุน
ที่เหมาะสมแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อให้สามารถปฏิบัติตามหน้าที่ของตนได้ง่ายกว่า

* 1. อาจแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรายเดียวสำหรับหน่วยงานภายใต้
	กรมควบคุมโรคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยที่แต่ละหน่วยงานภายในกลุ่มจะต้องสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย (มาตรา 41 วรรค 2) พระราชบัญญัติกำหนด
	ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้ติดต่อสำหรับเจ้าของข้อมูลส่วนบุคคลและหน่วยงานกำกับดูแล รวมถึงภายในองค์กรด้วย
1. **หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะมีหน้าที่ต่อไปนี้
	1. ให้คำแนะนำแก่กรมควบคุมโรค รวมทั้งลูกจ้างหรือผู้ให้บริการของผู้ควบคุมข้อมูล
	ส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัติ (อ้างอิงตามมาตรา 42 (1))
	2. ตรวจสอบการดำเนินงานของกรมควบคุมโรค รวมทั้งลูกจ้างหรือผู้ให้บริการของกรมควบคุมโรค เกี่ยวกับกิจกรรมที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและกิจกรรมอื่น ๆ ที่อาจเกี่ยวข้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าว (อ้างอิงตามมาตรา 42 (2))
	3. ประสานงานและให้ความร่วมมือกับหน่วยงานที่มีอำนาจในกรณีที่มีปัญหาเกี่ยวกับ
	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงพนักงานหรือผู้ให้บริการของกรมควบคุมโรค (อ้างอิงตามมาตรา 42 (3)) และ
	4. รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เนื่องจากการปฏิบัติหน้าที่ (อ้างอิงตามมาตรา 42 (4))

**อย่างไรก็ดี นอกจากหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 42 แล้ว อาจมีหน้าที่และความรับผิดชอบอื่นด้วย ดังต่อไปนี้**

ก) ตรวจสอบและทำให้มั่นใจว่าโปรแกรมและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด
ของกรมควบคุมโรค ซึ่งรวมถึงกรอบการดำเนินงานด้านความเป็นส่วนตัว กฎ นโยบาย แนวทางปฏิบัติ ประกาศ แบบคำขอความยินยอม สัญญา ฯลฯ และการบังคับใช้และการใช้สิ่งดังกล่าวเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายลำดับรอง แนวทางปฏิบัติ หรือคำสั่งที่ออกโดยอาศัยอำนาจของพระราชบัญญัติหรือกฎหมายอื่น ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

ข) ทำงานร่วมกับตัวแทนของหน่วยธุรกิจ/ฝ่ายงานหลักที่เกี่ยวข้องกับการประมวลผลข้อมูล
ส่วนบุคคล อย่างสม่ำเสมอเพื่อเฝ้าดูแลให้มีการปฏิบัติตามพระราชบัญญัติ หรือตรวจสอบและประเมิน
ความเสี่ยงเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองส่วนบุคคล

ค) สนับสนุนทีมธุรกิจทั้งหมดในการตัดสินใจที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

ง) ประเมินความเสี่ยงและวางแผน/เสนอแนะแผนในการรับมือกับความเสี่ยงที่เกี่ยวข้อง
กับความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล

จ) ให้ความรู้และ/หรือทำการฝึกอบรมพนักงานเกี่ยวกับการปฏิบัติตามพระราชบัญญัติตามที่จำเป็นและสม่ำเสมอ โดยมีจุดมุ่งหมายเพื่อสร้างและดำรงรักษาวัฒนธรรมการปฏิบัติตามกฎภายในกรมควบคุมโรค

ฉ) ดำเนินการจัดฝึกอบรมสำหรับพนักงานหรือลูกจ้างที่เกี่ยวข้องโดยตรงกับการประมวลผลข้อมูล
ส่วนบุคคลตามที่จำเป็น

ช) ทำหน้าที่เป็นผู้ติดต่อสำหรับกิจกรรมภายในกรมควบคุมโรคที่เกี่ยวข้องกับการประมวลผลข้อมูล
ส่วนบุคคลทั้งหมด เช่น วางกรอบในการจัดการคำขอของเจ้าของข้อมูลส่วนบุคคลจากเจ้าของข้อมูล
ส่วนบุคคล การปรึกษาหารือเกี่ยวกับปัญหาด้านการปฏิบัติตามกฎ ฯลฯ

ซ) ทำให้มั่นใจว่ามีการติดตามและการบันทึกข้อมูลเกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด และมีการดำเนินการต่าง ๆ ที่แสดงให้เห็นว่ากรมควบคุมโรคปฏิบัติตามพระราชบัญญัติและกฎหมายอื่น
ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

ฌ) ทำการประเมินและตรวจสอบการปฏิบัติตามพระราชบัญญัติเป็นประจำ

1. **หน้าที่ของกรมควบคุมโรคที่เกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**
	1. ต้องให้ข้อมูลและรายละเอียดติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและตัวแทน
	(เช่น ในเว็บไซต์ ในนโยบายความเป็นส่วนตัว ฯลฯ) และจะต้องแจ้งรายละเอียดเหล่านี้ต่อหน่วยงานกำกับดูแล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) และเจ้าของข้อมูลส่วนบุคคล (มาตรา 41 วรรค 5)
	2. ต้องดำเนินการต่อไปนี้
		1. ให้ความช่วยเหลือสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูล
		ส่วนบุคคล (เช่น ให้ทรัพยากรที่จำเป็นในการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 42 วรรค 2) และ
		2. ไม่เลิกจ้างหรือลงโทษเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ของตน (มาตรา 42 วรรค 3)
	3. ต้องรับรองกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่า หน้าที่หรือภารกิจอื่น ๆ ที่ปฏิบัติตามขอบเขตงาน ไม่ขัดกับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติ (มาตรา 42 วรรค 4)

**หมายเหตุ**

**การพิจารณาการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**

ภายใต้มาตรา 41 จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อ

* 1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่ คณะกรรมการประกาศกำหนด
	2. การดำเนินกิจกรรมของผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
	3. กิจกรรมหลักของผู้ประมวลผลข้อมูลส่วนบุคคลเป็น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

เมื่อพิจารณาดูแต่ละประเด็น ให้ใช้การวิเคราะห์และการประเมินต่อไปนี้

ก) การตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ : ประเด็นแรกที่ต้องพิจารณาคือ ทำการตรวจสอบเจ้าของข้อมูลส่วนบุคคล (เช่น ลูกค้า พันธมิตร ทางธุรกิจ และพนักงาน) อย่างสม่ำเสมอและเป็นระบบหรือไม่

ข) ข้อมูลจำนวนมาก : ประเด็นที่สองที่ต้องพิจารณาคือ ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นจำนวนมากหรือไม่ ทั้งนี้ พระราชบัญญัติยังไม่ได้กำหนดนิยามของคำว่า “จำนวนมาก” และไม่ได้กำหนดตัวเลขที่แน่นอนของปริมาณข้อมูลที่ทำการเก็บรวบรวม ใช้ หรือเปิดเผย หรือจำนวนบุคคลที่เกี่ยวข้อง

ค) การเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) :ประเด็นที่สามที่ต้องพิจารณาคือ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่มีความละเอียดอ่อนหรือไม่

ง) กิจกรรมหลักของหน่วยงาน : ประเด็นสุดท้ายที่ต้องพิจารณาคือการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวถือเป็นส่วนหนึ่งของกิจกรรมหลักของหน่วยงานหรือไม่

สรุปได้ว่า หากดำเนินการตรวจสอบข้อมูลส่วนบุคคลในจำนวนมากอย่างสม่ำเสมอและเป็นระบบ หรือหากกิจกรรมหลักเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล