



คู่มือปฏิบัติงานการคุ้มครองข้อมูลส่วนบุคคล ศูนย์คุณธรรม (องค์การมหาชน)

1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“กฎหมายคุ้มครองข้อมูลส่วนบุคคล”) ซึ่งมีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 โดย (ต่อไปในคู่มือปฏิบัตินี้เรียกว่า “ศูนย์คุณธรรม (องค์การมหาชน) หรือ ศคธ.”) ได้เห็นถึงความสำคัญของการกำหนดแนวทางในการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคล ศคธ. กำหนดกรอบการทำงาน เป็นขั้นตอนการปฏิบัติงานของผู้ที่เกี่ยวข้องในการจัดการข้อมูลส่วนบุคคล จากเจ้าของข้อมูลส่วนบุคคล ประกอบด้วย ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) สิทธิของเจ้าของข้อมูล (Data Subject Rights) การจัดการความปลอดภัยของข้อมูล (Data Security) การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office – DPO) เพื่อมุ่งเน้นถึงหน้าที่และความรับผิดชอบในการกระทำการใด ๆ ที่เกี่ยวข้องกับ ข้อมูลส่วนบุคคล และเพื่อให้มั่นใจว่า ศคธ. ตระหนักและเข้าใจถึงการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเป็นแนวทาง ในการนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลไปถือปฏิบัติโดยให้เป็นมาตรฐานเดียวกันทั้งหน่วยงาน

2. คำนิยาม

ลำดับที่	คำ	ความหมาย
1	ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
2	ข้อมูลส่วนบุคคลอ่อนไหว	ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพหรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด และที่แก้ไขเพิ่มเติม
3	เจ้าของข้อมูลส่วนบุคคล	บุคคลธรรมดา ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ ศคธ. เก็บ รวบรวม ใช้ หรือเปิดเผย เช่น ผู้สมัคร พนักงาน ลูกค้า ผู้ถือหุ้น คู่ค้า ผู้ให้บริการ และผู้มีส่วนได้เสียกับ ศคธ.
4	ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
5	ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคล ซึ่งดำเนินการดังกล่าว ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

6	เจ้าหน้าที่ คุ้มครองข้อมูล ส่วนบุคคล (DPO)	ผู้ปฏิบัติงาน ศคธ. ที่ได้รับการแต่งตั้ง/มอบหมายจากผู้อำนวยการ เพื่อทำหน้าที่ตรวจสอบ กำกับและให้คำแนะนำในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7	การประมวลผล ข้อมูลส่วนบุคคล	การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น เก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา การรับพิจารณา ใช้ ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผยด้วยการส่งต่อ เผยแพร่ โอน รวม หรือการกระทำอื่นใด ซึ่งทำให้เกิดความพร้อมใช้งาน การกำจัด การลบ หรือการทำลาย เป็นต้น
8	ผู้เยาว์	บุคคลอายุต่ำกว่า 20 ปี ที่ยังไม่บรรลุนิติภาวะโดยการสมรส หรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว ตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์
9	ผู้ไร้ความสามารถ	บุคคลวิกลจริต และศาลได้สั่งให้เป็นคนไร้ความสามารถ ซึ่งต้องจัดให้อยู่ในความอนุบาล
10	ผู้เสมือนไร้ความ สามารถ	บุคคลมีกายพิการ มีจิตใจฟั่นเฟือนไม่สมประกอบ หรือประพฤตีสุรุ่ยสุร่ายเสเพลเป็นอาชญา หรือติดสุรายาเมาหรือมีเหตุอื่นใดทำนองเดียวกันนั้น จนไม่สามารถจะจัดทำกรงานโดยตนเองได้ หรือจัดกิจการไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือครอบครัว และศาลได้สั่งให้เป็นคนเสมือนไร้ความสามารถ ซึ่งต้องจัดให้อยู่ในความพิทักษ์
11	ผู้ใช้อำนาจ ปกครอง	ตัวแทนบุตรและมีอำนาจทำการใด ๆ รวมทั้งทำนิติกรรมแทนบุตรได้ แต่ก็มีข้อจำกัดบางอย่างที่ผู้ใช้อำนาจปกครองจะทำเองไม่ได้แต่ต้องได้รับความ ยินยอมของบุตรก่อน จึงจะทำได้ อาทิ บิดามารดาผู้ให้กำเนิด หรือผู้เลี้ยงดู
12	ผู้อนุบาล	บุคคลซึ่งศาลมีคำสั่งแต่งตั้งให้เป็นผู้ปกครองดูแลคนไร้ความสามารถ
13	ผู้พิทักษ์	บุคคลซึ่งศาลมีคำสั่งแต่งตั้งให้เป็นผู้ปกครองดูแลคนเสมือนไร้ความสามารถ
14	การรั่วไหลของข้อมูล ส่วนบุคคล	การรั่วไหล หรือการละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคล การส่งผ่านข้อมูลส่วนบุคคลจากภายในหน่วยงานไปยังภายนอกหน่วยงานทำให้เกิดความเสี ยหาย การถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึงส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่น โดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล
15	สำนักงาน	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
16	ศคธ.	ศูนย์คุ้มครอง (องค์การมหาชน)

3. แนวทางปฏิบัติงานการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคล

3.1 วัตถุประสงค์

แนวทางปฏิบัติงานการขอความยินยอมของเจ้าของข้อมูลส่วนบุคคลจัดทำขึ้น เพื่อให้ความสำคัญในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยให้ผู้เกี่ยวข้องใช้เป็นแนวทางในการปฏิบัติงานเกี่ยวกับกระบวนการจัดการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล การจัดเก็บความยินยอมของเจ้าของข้อมูลส่วนบุคคล และการใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้หน่วยงานประมวลผลตามวัตถุประสงค์ที่ได้แจ้งไว้ รวมถึงการขอเพิกถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

3.2 ผู้รับผิดชอบ และหน้าที่ความรับผิดชอบ

ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ความรับผิดชอบ ดังนี้

- 1) แจ้งวัตถุประสงค์ของการจัดเก็บ ใช้งาน และการเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลทราบ
- 2) แจ้งวัตถุประสงค์ที่เพิ่มเติมหรือเปลี่ยนแปลงแก่เจ้าของข้อมูลส่วนบุคคลทราบ
- 3) พิจารณาความเป็นผู้เยาว์ ความเป็นผู้ไร้ความสามารถหรือความเป็นผู้เสมือนไร้ความสามารถของเจ้าของข้อมูลส่วนบุคคล
- 4) ขอความยินยอมจากเจ้าของข้อมูล
- 5) ขอความยินยอมจากผู้ใช้อำนาจปกครอง กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์
- 6) ขอความยินยอมจากผู้อุปถัมภ์ กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้ไร้ความสามารถ
- 7) ขอความยินยอมจากผู้พิทักษ์ กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เสมือนไร้ความสามารถ
- 8) ตรวจสอบการยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล หรือผู้มีอำนาจกระทำการแทน เจ้าของข้อมูลส่วนบุคคล
- 9) จัดเก็บผลการยินยอมทั้งที่ยินยอมและปฏิเสธ
- 10) แจ้งความยินยอมแก่ฝ่ายงานที่เกี่ยวข้อง

3.3 การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

3.3.1 ขั้นตอนปฏิบัติงานต่อข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บังคับใช้ (อ้างอิงตามมาตรา 95 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562) ศคธ.สามารถจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่ได้รวบรวมไว้ก่อนที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บังคับใช้ได้ ซึ่งต้องดำเนินการภายใต้วัตถุประสงค์เดิมและจะต้องแจ้งวิธีการเพิกถอนความยินยอมให้เจ้าของข้อมูลที่ไม่ประสงค์ให้เก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลรับทราบ

3.3.2 ขั้นตอนปฏิบัติต่อการขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลหลังที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บังคับใช้ (อ้างอิงตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

ขั้นตอนที่	รายละเอียด
1	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยินยอมด้วยตนเอง โดยใช้นโยบายการยินยอมด้วยตนเองตาม ข้อ 3.6 นโยบายการยินยอมด้วยตนเอง
2	เจ้าของข้อมูลส่วนบุคคล แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยินยอมด้วยตนเองเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 3.1) กรณีผลการพิจารณายินยอมด้วยตนเองถูกต้อง ให้ดำเนินการขั้นตอนที่ 4 3.2) กรณีผลการพิจารณายินยอมด้วยตนเองไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยินยอมด้วยตนเองไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
4	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งวัตถุประสงค์ของการจัดเก็บ และการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลรับทราบ ผ่านช่องทางที่เหมาะสม และเจ้าของข้อมูลส่วนบุคคล สามารถเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ ศคธ. (www.moralcenter.or.th) แอปพลิเคชัน เอกสาร หรือป้ายประกาศต่าง ๆ เป็นต้น โดยหากมีการใช้หรือประมวลผลข้อมูลส่วนบุคคล โดยบุคคลที่สามจะต้องมีการระบุรายละเอียดดังต่อไปนี้ 4.1) ข้อมูลส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่จะมีการใช้ร่วมกัน 4.2) ระบุชื่อบุคคลที่สามที่ใช้ข้อมูลส่วนบุคคลร่วมกันให้ชัดเจน 4.3) เหตุผลของการใช้ข้อมูลส่วนบุคคลร่วมกัน
5	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะให้ความยินยอมในการใช้ เปิดเผย หรือจัดเก็บ ตามวัตถุประสงค์ตามที่ ศคธ. แจ้งหรือไม่
6	ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือไม่ยินยอม 6.1) กรณียินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) 6.2) กรณีไม่ยินยอม: ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

3.3.3 ขั้นตอนปฏิบัติงานต่อการเปิดเผยหรือเปลี่ยนแปลงวัตถุประสงค์ในการใช้งาน (อ้างอิงตามมาตรา 19 และ 21 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

ขั้นตอนที่	รายละเอียด
1	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยินยอมด้วยตนเอง โดยใช้นโยบายการยินยอมด้วยตนเองตาม ข้อ 3.6 นโยบายการยินยอมด้วยตนเอง
2	เจ้าของข้อมูลส่วนบุคคล แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยินยอมด้วยตนเองเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 3.1) กรณีผลการพิจารณายินยอมด้วยตนเองถูกต้อง ให้ดำเนินการขั้นตอนที่ 4

	3.2) กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
4	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งประกาศความเป็นส่วนตัว (Privacy Notice) ให้แก่ เจ้าของข้อมูลส่วนบุคคลที่ ศคธ. ได้จัดเก็บข้อมูลส่วนบุคคลไว้ให้ทราบผ่านช่องทางที่เหมาะสม และเจ้าของข้อมูลส่วนบุคคลเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ ศคธ. แอปพลิเคชัน เอกสาร หรือป้ายประกาศต่าง ๆ เป็นต้น เมื่อมีการเปิดเผยหรือเปลี่ยนแปลงวัตถุประสงค์ในการใช้งาน
5	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งวัตถุประสงค์ของการจัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่เพิ่มเติมหรือเปลี่ยนแปลงให้เจ้าของข้อมูลส่วนบุคคลรับทราบผ่านช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้สะดวก ตามที่ได้ระบุไว้ในขั้นตอนที่ 4 ในกรณีมีการใช้ หรือประมวลผลข้อมูลส่วนบุคคล โดยบุคคลที่สามจะต้องมีการระบุนายละเอียดดังต่อไปนี้ 5.1) ข้อมูลส่วนตัวของเจ้าของส่วนบุคคลที่จะมีการใช้ร่วมกัน 5.2) ระบุชื่อบุคคลที่สามที่ใช้ข้อมูลส่วนบุคคลร่วมกันให้ชัดเจน 5.3) เหตุผลของการใช้ข้อมูลส่วนบุคคลร่วมกัน
6	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะให้ความยินยอมการจัดเก็บ หรือประมวลผลข้อมูลตามวัตถุประสงค์ที่ ศคธ. แจ้งหรือไม่
7	ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึก และจัดเก็บเกี่ยวกับความยินยอม หรือไม่ยินยอม 7.1) กรณียินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูล ส่วนบุคคลได้ที่ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) 7.2) กรณีไม่ยินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ที่ไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

3.3.4 ขั้นตอนปฏิบัติงานต่อการขอความยินยอมจากผู้เยาว์ (อ้างอิงตามมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรา 22, 23, 24 จากประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ. 2535)

ขั้นตอนที่	รายละเอียด
1	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยืนยันตัวตน โดยใช้แนวปฏิบัติการยืนยันตัวตนตาม ข้อ 3.6 แนวปฏิบัติการยืนยันตัวตน
2	เจ้าของข้อมูลส่วนบุคคล แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 3.1) กรณีผลการพิจารณายืนยันตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 4 3.2) กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
4	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์หรือไม่ 4.1) กรณีที่เป็นผู้เยาว์: ให้ดำเนินการขั้นตอนที่ 5 4.2) กรณีที่ไม่ใช่ผู้เยาว์: ให้ดำเนินการตามข้อ 3.3.2 ขั้นตอนปฏิบัติการขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคล

5	<p>ผู้ควบคุมข้อมูลส่วนบุคคล กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์: ให้ดำเนินการดังต่อไปนี้</p> <p>5.1) กรณีที่ผู้เยาว์มีอายุไม่เกิน 10 ปี: ต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจ กระทำการแทนผู้เยาว์</p> <p>5.2) กรณีที่ผู้เยาว์มีอายุเกิน 10 ปี แต่ไม่เกิน 20 ปี: ให้ขอความยินยอมจากผู้เยาว์โดยที่ผู้เยาว์ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองในการให้ความยินยอมต่อ ศคธ.</p> <p>5.3) ผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือหลุดพ้นจากหน้าที่อันใดอันหนึ่ง หรือต้องทำเองเฉพาะตัว หรือเป็นการสมควรแก่ฐานะ และจำเป็นต่อการดำรงชีพตามสมควร และให้ดำเนินการขั้นตอนที่ 7</p>
6	<p>กรณีผู้เยาว์ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง: ให้ดำเนินการดังต่อไปนี้</p> <p>6.1) ผู้ควบคุมข้อมูลส่วนบุคคล</p> <p>ขอหลักฐานการแสดงความเป็นผู้ใช้อำนาจปกครองและแจ้งความประสงค์ให้ผู้ใช้อำนาจปกครองยืนยันตัวตน</p> <p>6.2) ผู้ใช้อำนาจปกครอง ต้องดำเนินการดังนี้</p> <p>6.2.1) แสดงหลักฐานความเป็นผู้ใช้อำนาจปกครอง</p> <ul style="list-style-type: none"> - กรณีบิดามารดาผู้ให้กำเนิด: ต้องยื่นหลักฐานประกอบ ได้แก่ สูติบัตร หรือสำเนาบัตรประชาชน และทะเบียนบ้าน เป็นต้น - กรณีไม่ใช่บิดามารดาผู้ให้กำเนิด: ต้องยื่นหลักฐานการเลี้ยงดูประกอบ ได้แก่การจ่ายค่าเทอม <p>หลักฐานการยืนยันการเลี้ยงดูจากกรมการปกครอง เป็นต้น</p> <p>6.2.2) แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูลเพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล พร้อมเอกสารหลักฐาน</p>
7	<p>ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่</p> <p>7.1) กรณีผลการพิจารณายืนยันตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 8</p> <p>7.2) กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จหรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ</p>
8	<p>ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ให้แก่ เจ้าของข้อมูลส่วนบุคคลที่ ศคธ. ได้จัดเก็บข้อมูลส่วนบุคคลไว้ได้ทราบผ่านช่องทางที่เหมาะสม และเจ้าของข้อมูลส่วนบุคคลเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ ศคธ. แอปพลิเคชัน เอกสาร หรือป้ายประกาศต่าง ๆ เป็นต้น</p>
9	<p>เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะให้ความยินยอมการจัดเก็บ หรือประมวลผลข้อมูลตามวัตถุประสงค์ที่ ศคธ. แจ้งหรือไม่</p>
10	<p>ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือความไม่ยินยอม</p> <p>10.1) กรณีที่เป็นผู้เยาว์: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือ แสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ที่ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสารตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)</p> <p>10.2) กรณีที่ไม่ใช่ผู้เยาว์: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคล ได้ที่ไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสารตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)</p>

3.3.5 ขั้นตอนปฏิบัติงานต่อการขอความยินยอมจากเจ้าของข้อมูลประเภทผู้ไร้ความสามารถ (อ้างอิงตามมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรา 28 จากประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ. 2535)

ขั้นตอนที่	รายละเอียด
1	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยินยอมตัวตน โดยใช้แนวปฏิบัติการยินยอมตัวตนตามข้อ 3.6 แนวปฏิบัติการยินยอมตัวตน
2	เจ้าของข้อมูลส่วนบุคคล แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยินยอมตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 3.1) กรณีผลการพิจารณายินยอมตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 4 3.2) กรณีผลการพิจารณายินยอมตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยินยอมตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
4	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาเจ้าของข้อมูลส่วนบุคคลเป็นผู้ไร้ความสามารถหรือไม่ 4.1) กรณีที่เป็นผู้ไร้ความสามารถ: ต้องขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนผู้ไร้ความสามารถผู้นั้น 4.2) กรณีที่ไม่ใช่ผู้ไร้ความสามารถ: ให้ดำเนินการตามข้อ 3.3.2 ขั้นตอนปฏิบัติการขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลใหม่
5	กรณีผู้ไร้ความสามารถต้องได้รับความยินยอมจากผู้อนุบาล: ให้ดำเนินการดังต่อไปนี้ 5.1) ผู้ควบคุมข้อมูลส่วนบุคคล ขอหลักฐานความเป็นผู้อนุบาล และแจ้งความประสงค์ให้ผู้อนุบาลยินยอมตัวตน 5.2) ผู้อนุบาลต้องดำเนินการดังนี้ 5.2.1) แสดงหลักฐานความเป็นผู้อนุบาล ได้แก่ คำสั่งศาลแต่งตั้งให้เป็นผู้อนุบาลคนไร้ความสามารถ 5.2.2) แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูลเพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
6	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยินยอมตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 6.1) กรณีผลการพิจารณายินยอมตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 7 6.2) กรณีผลการพิจารณายินยอมตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยินยอมตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
7	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ให้แก่เจ้าของข้อมูลส่วนบุคคลที่ ศคธ. ได้จัดเก็บข้อมูลส่วนบุคคลไว้ได้ทราบผ่านช่องทางที่เหมาะสมและเจ้าของข้อมูลส่วนบุคคลเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ ศคธ. แอปพลิเคชัน เอกสารหรือป้ายประกาศต่าง ๆ เป็นต้น
8	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะให้ความยินยอมการจัดเก็บ หรือประมวลผลข้อมูลตามวัตถุประสงค์ที่ ศคธ. แจ้งหรือไม่
9	ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บเกี่ยวกับความยินยอมหรือไม่ยินยอม

3.3.6 ขั้นตอนปฏิบัติงานต่อการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลประเภทผู้เสมือนไร้ความสามารถ (อ้างอิงจากมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรา 32 จากประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ. 2535)

ขั้นตอนที่	รายละเอียด
1	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งความประสงค์ให้เจ้าของข้อมูลส่วนบุคคลยินยอมตัวตน โดยใช้แนวปฏิบัติการยินยอมตัวตนตามข้อ 3.6 แนวปฏิบัติการยินยอมตัวตน
2	เจ้าของข้อมูลส่วนบุคคล แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูล เพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
3	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยินยอมตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 3.1) กรณีผลการพิจารณายินยอมตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 4

	3.2) กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
4	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาเจ้าของข้อมูลเป็นผู้เสมือนไร้ความสามารถหรือไม่ 4.1) กรณีที่เป็นผู้เสมือนไร้ความสามารถ: ต้องขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนผู้ไร้ความสามารถผู้นั้น 4.2) กรณีที่ไม่ใช่ผู้เสมือนไร้ความสามารถ: ให้ดำเนินการตามข้อ 3.3.2 ขั้นตอนปฏิบัติการขอความยินยอมเปิดเผยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลใหม่
5	กรณีผู้เสมือนไร้ความสามารถต้องได้รับความยินยอมจากผู้พิทักษ์: ให้ดำเนินการดังต่อไปนี้ 5.1) ผู้ควบคุมข้อมูลส่วนบุคคล ขอหลักฐานความเป็นผู้พิทักษ์ และแจ้งความประสงค์ให้ผู้พิทักษ์ยืนยันตัวตน 5.2) ผู้พิทักษ์ ต้องดำเนินการดังนี้ 5.2.1) แสดงหลักฐานความเป็นผู้พิทักษ์ ได้แก่ คำสั่งศาลแต่งตั้งให้เป็นผู้พิทักษ์คนเสมือนไร้ความสามารถ 5.2.2) แสดงข้อมูลหรือแจ้งรายละเอียดข้อมูลเพื่อยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคล
6	ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการยืนยันตัวตนเจ้าของข้อมูลส่วนบุคคลว่าสำเร็จ ถูกต้องหรือไม่ 6.1) กรณีผลการพิจารณายืนยันตัวตนถูกต้อง ให้ดำเนินการขั้นตอนที่ 7 6.2) กรณีผลการพิจารณายืนยันตัวตนไม่สำเร็จ หรือไม่ถูกต้อง ให้แจ้งผลการยืนยันตัวตนไม่สำเร็จให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และให้ถือว่าสิ้นสุดกระบวนการ
7	ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) ให้แก่เจ้าของข้อมูลส่วนบุคคลที่ ศคธ. ได้จัดเก็บข้อมูลส่วนบุคคลไว้ได้ทราบผ่านช่องทางที่เหมาะสมและเจ้าของข้อมูลส่วนบุคคลเข้าถึงได้สะดวก เช่น บนเว็บไซต์ของ ศคธ. แอปพลิเคชัน เอกสารหรือป้ายประกาศต่าง ๆ เป็นต้น
8	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะให้ความยินยอมการจัดเก็บ หรือประมวลผลข้อมูลตามวัตถุประสงค์ที่ ศคธ. แจ้งหรือไม่
9	ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือไม่ยินยอม 9.1) กรณียินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ที่ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ได้ระบุ ไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) 9.2) กรณีไม่ยินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ที่ไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ได้ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

3.3.7 ขั้นตอนปฏิบัติงานต่อการขอความยินยอมผ่านคุกกี้ (Cookies)

ขั้นตอนที่	รายละเอียด
1	เจ้าของข้อมูลส่วนบุคคล เข้าสู่หน้าเว็บไซต์ของ ศคธ. www.moralcenter.or.th
2	ผู้ควบคุมข้อมูลส่วนบุคคล โดยเว็บไซต์ของ ศคธ. แสดงแถบการยอมรับคุกกี้ (Cookie Consent Banner) ที่แจ้งวัตถุประสงค์การจัดเก็บ ใช้งานข้อมูลของคุกกี้ กรณีมีหลายวัตถุประสงค์ จะต้องแยกความยินยอมเป็นรายวัตถุประสงค์ เพื่อให้เจ้าของข้อมูลส่วนบุคคลพิจารณายืนยัน หรือปฏิเสธความยินยอมเป็นรายวัตถุประสงค์บนหน้าเว็บไซต์
3	เจ้าของข้อมูลส่วนบุคคล พิจารณาว่าจะยินยอมให้ ศคธ.

	จัดเก็บใช้งานข้อมูลคุกคามของเจ้าของข้อมูลส่วนบุคคลในฐานะผู้ใช้งานหรือไม่
4	<p>ผู้ควบคุมข้อมูลส่วนบุคคล ทำการบันทึกและจัดเก็บ เกี่ยวกับความยินยอมหรือไม่ยินยอม</p> <p>4.1) กรณียินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือแสดงความยินยอม เอกสารการแสดงความยินยอม</p> <p>หรือข้อมูลความยินยอมของเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ในระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาในการจัดเก็บให้เป็นตามที่ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)</p> <p>4.2) กรณีไม่ยินยอม: ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องบันทึก และ/หรือจัดเก็บหนังสือเอกสาร หรือข้อมูลการปฏิเสธความยินยอมของเจ้าของข้อมูลส่วนบุคคล ได้ที่ไว้ใน ระบบอิเล็กทรอนิกส์ (ถ้ามี) หรือเข้าแฟ้มเอกสาร ตามช่องทางที่ได้รับการปฏิเสธจากเจ้าของ ข้อมูลส่วนบุคคล ทั้งนี้ ระยะเวลาการจัดเก็บให้เป็นตามที่ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)</p> <p>4.3) กรณีที่ไม่ได้ระบุความยินยอม: ให้ระบบแจ้งวัตถุประสงค์ การจัดเก็บการใช้งานข้อมูลคุกคาม อีกครั้ง</p>

3.4 ขั้นตอนปฏิบัติงานต่อการจัดเก็บความยินยอม

ขั้นตอนที่	รายละเอียด
1	จัดทำแบบฟอร์มการขอความยินยอมแยกตามประเภท ขอบเขต หรือตามที่ได้มีการปรับปรุงเนื้อหาในแบบฟอร์มดังกล่าว เพื่อไม่ให้กระทบฟอร์มเดิมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ผลการยินยอมไว้ และสามารถตรวจสอบ และเปรียบเทียบได้
2	<p>ทำการบันทึกเนื้อหา และข้อมูล หลังเสร็จสิ้นกระบวนการการขอความยินยอม ดังนี้</p> <p>2.1) ชุดเนื้อหาข้อมูลการขอความยินยอม</p> <p>2.2) วิธีการให้ความยินยอม</p> <p>2.3) สถานะยินยอม หรือไม่ยินยอมตามรายการวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้แจ้งไว้</p> <p>2.4) เอกสารที่เป็นกระดาษ หรือรูปแบบอิเล็กทรอนิกส์ฟอร์มที่ใช้บันทึก (ถ้ามี)</p>
3	รวบรวมจัดเก็บความยินยอมที่ได้รับ ผ่านช่องทางต่าง ๆ ไว้ ณ ที่จัดเตรียมไว้ภายใต้มาตรการรักษาความปลอดภัยที่เพียงพอ ไม่ว่าจะ เป็นระบบอิเล็กทรอนิกส์หรือแฟ้มเอกสาร ซึ่งเป็นกระดาษที่เก็บรักษาไว้ในสถานที่มั่นคงปลอดภัย
4	กำหนดการตรวจสอบ ทบทวน ความเหมาะสมและขอบเขตของความยินยอมให้ทันสมัย และเป็นปัจจุบัน

3.5 ขั้นตอนปฏิบัติงานต่อการขอเพิกถอนความยินยอมการใช้ เปิดเผยข้อมูลส่วนบุคคล

ขั้นตอนที่	รายละเอียด
1	<p>ศคธ. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการดังนี้</p> <p>1.1) แจ้งเจ้าของข้อมูลส่วนบุคคลถึงสิทธิการขอเพิกถอนความยินยอมในการใช้ เปิดเผยข้อมูล ส่วนบุคคล โดยสามารถกระทำได้ตลอดเวลา และง่ายต่อการเพิกถอนความยินยอม</p> <p>1.2) แจ้งขั้นตอนสำหรับการขอเพิกถอนความยินยอมดังกล่าว รวมถึงการอ้างอิงใด ๆ ต่อข้อผูกพันทางกฎหมาย หรือทางกฎหมายที่อาจยังคงมีผลบังคับใช้แม้หลังจากเจ้าของข้อมูลส่วนบุคคลได้ทำการเพิกถอนความยินยอม</p> <p>1.3) แจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบว่าการขอเพิกถอนความยินยอมดังกล่าวจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลได้</p>
2	เมื่อเจ้าของข้อมูลส่วนบุคคลแสดงความประสงค์การขอเพิกถอนความยินยอม ให้หน่วยงานปฏิบัติตาม

	แนวทางปฏิบัติงานการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ศูนย์คุณธรรม (องค์การมหาชน)
3	ให้กำหนดวิธีการในการขอเพิกถอนความยินยอม โดยใช้ช่องทางและรูปแบบเดียวกันกับเมื่อตอนแสดงการร้องขอความยินยอม เพื่อให้กระบวนการสอดคล้องกัน และสามารถตรวจสอบได้

3.6 แนวปฏิบัติการยืนยันตัวตน

ศคธ. กำหนดแนวปฏิบัติการยืนยันตัวตน

โดยเจ้าของข้อมูลส่วนบุคคลต้องดำเนินการยืนยันตัวตนให้ถูกต้องอย่างน้อย 3 รายการแรก ดังนี้

- 1) ชื่อ
- 2) นามสกุล
- 3) เลขบัตรประจำตัวบัตรประชาชน
- 4) วัน เดือน ปี เกิด
- 5) ที่อยู่
- 6) หมายเลขโทรศัพท์
- 7) อีเมล

4. แนวทางปฏิบัติงานการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

4.1 วัตถุประสงค์

แนวทางปฏิบัติงานการจัดการคำร้องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลจัดทำขึ้น

เพื่อให้ผู้เกี่ยวข้องใช้เป็นแนวทางในการปฏิบัติงานเกี่ยวกับกระบวนการรับแบบคำร้อง การจัดการสิทธิคำร้อง รวมถึงการแจ้งใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลสำหรับ ศคธ.

4.2 ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

ลำดับที่	ผู้รับผิดชอบ	หน้าที่ความรับผิดชอบ
1	เจ้าหน้าที่ผู้รับเรื่อง	1) รับคำร้องขอของเจ้าของข้อมูล 2) ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ
2	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	1) พิจารณาความถูกต้องของคำร้องขอ 2) พิจารณาคำใช้จ่ายดำเนินการเพื่อปฏิบัติตามคำขอ (ถ้าจำเป็น) 3) แจ้งผลการขอใช้สิทธิ

3	ผู้ควบคุมข้อมูลส่วนบุคคล	1) ดำเนินการหรือไม่ดำเนินการตามคำร้อง 2) บันทึกผลการใช้หรือปฏิเสธการใช้สิทธิ 3) รายงานผลให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
---	--------------------------	---

4.3 ขั้นตอนปฏิบัติงานต่อการแจ้งใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(อ้างอิงตามมาตรา 30, 32, 33, 34, 35, 36, 37, 73 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรา 22, 23, 24, 28, 32 ตามประมวลกฎหมายแพ่งและพาณิชย์ พ.ศ. 2535)

ศคธ.ดำเนินการตามคำร้องของเจ้าของข้อมูลส่วนบุคคล

โดยผู้รับผิดชอบดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า ภายใน 30 วัน นับแต่ที่ได้รับคำขอ

ขั้นตอนที่	รายละเอียด
1	เจ้าของข้อมูลส่วนบุคคล ผู้ร้องขอแจ้งหรือผู้ยื่นคำร้องขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคล ผ่านช่องทางการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ ศคธ. กำหนด
2	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดำเนินการ ดังนี้ 2.1 รับคำขอจากเจ้าของข้อมูลส่วนบุคคล หรือผู้ยื่นคำร้องขอ ตามแบบคำร้องขอใช้สิทธิของ เจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) 2.2 แจ้งให้เจ้าของข้อมูลส่วนบุคคลหรือผู้ยื่นคำร้องทำการยืนยันตัวตน 2.3 พิจารณามอบหมายเจ้าหน้าที่ผู้รับเรื่องของแต่ละฝ่ายงาน ให้ความเห็นประกอบการพิจารณา (ถ้ามี)
3	เจ้าหน้าที่ผู้รับเรื่อง บันทึกรายละเอียดในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form)
4	เจ้าหน้าที่ผู้รับเรื่อง พิจารณายืนยันตัวตน โดยใช้แนวปฏิบัติการยืนยันตัวตนตาม ข้อ 4.7 แนวปฏิบัติการยืนยันตัวตน 4.1 กรณียืนยันตัวตนไม่สำเร็จ: เจ้าหน้าที่ผู้รับเรื่อง แจ้งผลยืนยันตัวตนของผู้ยื่นคำร้องขอใช้สิทธิไม่สำเร็จให้กับเจ้าของข้อมูลส่วนบุคคลหรือผู้ยื่นคำร้องขอ และให้ถือว่าสิ้นสุดกระบวนการ 4.2 กรณียืนยันตัวตนสำเร็จ: ให้ดำเนินการขั้นตอนที่ 5 ต่อไป
5	เจ้าหน้าที่ผู้รับเรื่อง ตรวจสอบผู้ยื่นคำร้องขอเป็นบุคคลอื่นที่ประสงค์กระทำการแทนเจ้าของข้อมูลส่วนบุคคลหรือไม่ 5.1 กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์: ผู้ยื่นคำร้องขอจะต้องเป็นผู้ใช้อำนาจปกครองกระทำแทนผู้เยาว์ โดยให้ดำเนินการดังต่อไปนี้ 5.1.1 หากเป็นบิดามารดาผู้ให้กำเนิด ผู้ยื่นคำร้องขอ ต้องยื่นหลักฐานสูติบัตร หรือสำเนาบัตรประชาชน พร้อมทั้งทะเบียนบ้าน 5.1.2 หากไม่ใช่บิดามารดาผู้ให้กำเนิด ผู้ยื่นคำร้องขอ ต้องยื่นหลักฐานการจ่ายค่าเทอม หลักฐานการยืนยันการเลี้ยงดูจากกรมการปกครอง เป็นต้น 5.2 กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้ไร้ความสามารถ:

	<p>ผู้ยื่นคำร้องขอจะต้องเป็นผู้อนุบาลกระทำแทนผู้ไร้ความสามารถ และผู้ยื่นคำร้องขอต้องยื่นหลักฐานคำสั่งศาลแต่งตั้งเป็นผู้อนุบาลของเจ้าของข้อมูลส่วนบุคคล</p> <p>5.3 กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เสมือนไร้ความสามารถ: ผู้ยื่นคำร้องขอต้องยื่นหลักฐานคำสั่งศาลแต่งตั้งเป็นผู้พิทักษ์ของเจ้าของข้อมูลส่วนบุคคล</p> <p>5.4 กรณีเจ้าของข้อมูลส่วนบุคคลเป็นบุคคลธรรมดา: เจ้าหน้าที่ผู้รับเรื่อง พิจารณาคำร้องในขั้นตอนที่ 7 ต่อไป</p>
6	<p>เจ้าหน้าที่ผู้รับเรื่อง ตรวจสอบหลักฐานแล้ว พบว่า</p> <p>6.1 กรณีหลักฐานไม่ถูกต้อง ให้แจ้งผู้ยื่นคำร้องขอทราบ และให้ถือว่าสิ้นสุดกระบวนการ</p> <p>6.2 กรณีหลักฐานถูกต้อง ให้เจ้าหน้าที่ผู้รับเรื่อง พิจารณาคำร้องในขั้นตอนที่ 7 ต่อไป</p>
7	<p>เจ้าหน้าที่ผู้รับเรื่อง พิจารณาคำร้องขอของเจ้าของข้อมูลส่วนบุคคลว่าถูกต้อง สมบูรณ์ หรือเป็นคำขอที่สมเหตุสมผลหรือไม่ หรือมีเหตุแห่งการปฏิเสธคำร้องขอนั้น ตาม ข้อ 4.5 เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอของเจ้าของข้อมูล หรือไม่</p> <p>7.1 กรณี ไม่สามารถดำเนินการได้ตามคำขอ ให้ดำเนินการดังต่อไปนี้</p> <p>7.1.1 เจ้าหน้าที่ผู้รับเรื่อง แจ้งเหตุผลการปฏิเสธคำร้องขอแก่เจ้าของข้อมูลส่วนบุคคล หรือผู้ร้องขอทราบ ตามหนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding)</p> <p>7.1.2 เจ้าหน้าที่ผู้รับเรื่อง</p> <p>บันทึกเหตุผลการปฏิเสธการปฏิบัติตามคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลหรือผู้ยื่นคำร้องลงในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่</p> <p>7.1.3 สิ้นสุดกระบวนการ</p> <p>7.2 กรณี สามารถดำเนินการได้ตามคำขอ ให้ดำเนินการตามขั้นตอนที่ 8 ต่อไป</p>
8	<p>เจ้าหน้าที่ผู้รับเรื่อง พิจารณาค่าใช้จ่ายกรณีที่มีการขอในรูปแบบเอกสารเป็นจำนวนมากต่อคำขอนั้น</p> <p>8.1 กรณีที่ไม่มีค่าใช้จ่าย ให้ดำเนินการดังต่อไปนี้</p> <p>8.1.1 เจ้าหน้าที่ผู้รับเรื่อง ดำเนินการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ที่เกี่ยวข้อง ดำเนินการตามคำขอ</p> <p>8.1.2 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ที่เกี่ยวข้อง ดำเนินการตามคำขอ และบันทึกรายละเอียดในระบบ</p> <p>8.1.3 เจ้าหน้าที่ผู้รับเรื่อง</p> <p>แจ้งผลการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคลหรือผู้ร้องขอทราบตามหนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding)</p> <p>และบันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ว่าคำขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</p> <p>8.1.4 สิ้นสุดกระบวนการ</p> <p>8.2 กรณีมีค่าใช้จ่าย: เนื่องจากเป็นคำร้องที่มีลักษณะเดิมซ้ำ ๆ โดยไม่มีเหตุอันควร หรือต้องส่งเป็นเอกสารให้แก่เจ้าของข้อมูลส่วนบุคคลในปริมาณที่มาก ทำให้เกิดค่าใช้จ่ายให้ดำเนินการดังต่อไปนี้</p> <p>8.2.1 เจ้าหน้าที่ผู้รับเรื่อง แจ้งเจ้าของข้อมูลส่วนบุคคลให้รับทราบค่าใช้จ่ายในการดำเนินการตามการใช้สิทธิ</p> <p>8.2.2 เจ้าของข้อมูลส่วนบุคคล พิจารณาการยืนยันการใช้สิทธิ:</p> <p>8.2.2.1 กรณี ยืนยันให้ดำเนินการต่อ</p>

<p>1) เจ้าหน้าที่ผู้รับเรื่อง รับทราบการยืนยันการขอใช้สิทธิ</p> <p>2) เจ้าหน้าที่ผู้รับเรื่อง แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือฝ่ายงานที่เกี่ยวข้อง ดำเนินการตามคำขอ</p> <p>3) ผู้ควบคุมข้อมูลส่วนบุคคลหรือฝ่ายงานที่เกี่ยวข้อง ดำเนินการตามคำขอและแจ้งผลการดำเนินการให้เจ้าหน้าที่ผู้รับเรื่อง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล</p> <p>4) เจ้าหน้าที่ผู้รับเรื่อง แจ้งผลการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคล หรือผู้ร้องขอทราบตามหนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Responding) ศคธ. และบันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ ว่าคำขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</p> <p>8.2.2.2 กรณี ไม่ให้ดำเนินการต่อ</p> <p>1) เจ้าหน้าที่ผู้รับเรื่อง รับทราบ การยกเลิกการขอใช้สิทธิ</p> <p>2) เจ้าหน้าที่ผู้รับเรื่อง บันทึกผลการดำเนินการในแบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Form) สำหรับเจ้าหน้าที่ ว่าคำขอดังกล่าว ได้มีการดำเนินการเป็นที่เรียบร้อยแล้ว</p>

4.4 สิทธิของเจ้าของข้อมูล

สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ได้รับการรับรองตามแนวปฏิบัติ ดังต่อไปนี้

- 1) สิทธิได้รับแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล
- 2) สิทธิในการเพิกถอนความยินยอม
- 3) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- 4) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- 5) สิทธิในการลบข้อมูลส่วนบุคคล
- 6) สิทธิในการระงับการประมวลผลข้อมูลส่วนบุคคล
- 7) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล
- 8) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล

4.5 เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล

คำขอไม่สมเหตุสมผล	คำขอ ฟุ่มเฟือย	เจ้าของข้อมูล มีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับกฎหมายการทำสัญญา	เกิดผลกระทบต่อผลประโยชน์แก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐหรือหน้าที่ตามกฎหมาย	ก่อตั้งใช้หรือป้องกันสิทธิทางกฎหมายโดยชอบ
1. การเพิกถอนความยินยอม	X	X	X	X	X	X	X	X
2.	✓	X	X	✓	X	X	X	X

การเข้าถึงข้อมูลส่วนบุคคล								
3. การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	X	X	X	X	X	X	X
4. การลบข้อมูลส่วนบุคคล	✓	X	X	X	X			X
5. การระงับการประมวลผลข้อมูลส่วนบุคคล	✓	X	X	X	X			X
6. การให้โอนย้ายข้อมูลส่วนบุคคล	✓	X	X	X	X	✓	X	X
7. การคัดค้านการประมวลผลข้อมูลส่วนบุคคล		X	X	X	✓	✓	✓	

หมายเหตุ:

✓ หมายถึง สามารถปฏิเสธคำร้องขอเจ้าของข้อมูล

X หมายถึง ไม่สามารถปฏิเสธคำร้องขอเจ้าของข้อมูล

4.6 ช่องทางการติดต่อสอบถามหรือยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

หากมีข้อสงสัย ข้อเสนอแนะ หรือข้อกังวลเกี่ยวกับเกี่ยวกับแนวทางปฏิบัติงานกรณีเกิดข้อร้องเรียน

การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล หรือต้องการแจ้งเหตุการณ์การละเมิดหรือ

การรั่วไหลของข้อมูลส่วนบุคคล สามารถติดต่อสอบถามได้ที่

1) ติดต่อด้วยตนเอง ณ ศูนย์คุณธรรม (องค์การมหาชน) 69 ชั้น 16-17 อาคารวิทยาลัยการจัดการ

มหาวิทยาลัยมหิดล แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400 เวลาทำการ (08:30 – 16:30 น.) วันจันทร์ -

วันศุกร์ (ยกเว้นวันหยุดที่ราชการกำหนด)

2) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail): info@moralcenter.or.th

3) โทรศัพท์: 0 2644 9900

5. คู่มือปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ

5.1 วัตถุประสงค์

คู่มือปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ

จัดทำขึ้นเพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคล

5.2 ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ความรับผิดชอบ ดังนี้

1) กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสารไม่ต้องดำเนินการตามคำร้องขอจนกว่าจะ

พิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริง หรือมีข้อยกเว้นตามกฎหมายประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)

2) ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ให้หน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลได้

ในกรณีที่หน่วยงานของรัฐมีอำนาจตามกฎหมายเท่านั้น หากหน่วยงานของรัฐไม่มีอำนาจตามกฎหมาย

ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการไม่ให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้น

ผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูล

โดยไม่มีหน้าที่ตามกฎหมาย

3) ผู้ประมวลผลข้อมูล ให้หน่วยงานของรัฐเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่หน่วยงานของรัฐมี

อำนาจตามกฎหมายเท่านั้น ในขณะที่เดียวกันผู้ประมวลผลข้อมูลต้องมีข้อผูกพันกับผู้ควบคุมข้อมูลส่วนบุคคล

ตามสัญญาหรือข้อตกลงว่าไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่นหากหน่วยงานของรัฐไม่มีอำนาจตาม

กฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้หน่วยงานของรัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้น

ผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมายและความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูลส่วนบุคคล

หากให้หน่วยงานของรัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวอีกด้วย

5.3 ขั้นตอนการปฏิบัติงานการจัดการคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานของรัฐ

ขั้นตอนที่	รายละเอียด
1	ผู้ยื่นคำร้อง ยื่นแบบคำร้องขอให้เปิดเผยข้อมูลแก่ ศคธ.
2	ผู้รับเรื่องคำร้อง พิจารณาคำร้องขอหรือคำสั่งโดยระบุหน่วยงานของรัฐ หรือเจ้าหน้าที่ผู้ร้องขอ โดยพิจารณาข้อมูล ดังนี้ <ul style="list-style-type: none"> - ชื่อ-นามสกุล เจ้าหน้าที่ และชื่อหน่วยงาน - วันที่ได้รับคำร้องขอ - ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย
3	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่ และมีข้อยกเว้นหรือไม่
4	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พิจารณาความถูกต้องแท้จริงของเอกสาร ดังนี้ <p>4.1 กรณี มีเอกสารมาแสดง:</p> <p>4.1.1 กรณีมีหมายศาล หรือคำสั่งศาล ให้ดำเนินการตามคำร้องขอในขั้นตอนที่ 5.1</p> <p>4.1.2 กรณีเอกสารอื่น ๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจ ตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไป หรืออำนาจ ที่บัญญัติไว้กว้าง ๆ ว่ามีอำนาจหน้าที่อื่นใด เพื่อให้การปฏิบัติหน้าที่บรรลุมิวัตถุประสงค์ (เช่นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 18(2) เรียกข้อมูลจากรคอมพิวเตอร์ เป็นต้น) หากพิจารณาแล้วมีความน่าเชื่อถือ และเห็นว่ามีความจำเป็นต้องเข้าถึงข้อมูลจริง ให้ดำเนินการตามคำร้องขอในขั้นตอนที่ 5.1 ต่อไป</p> <p>4.2 กรณี ไม่มีเอกสาร หรือมีข้อสงสัยเกี่ยวกับเอกสาร ไม่ต้องดำเนินการตามคำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจอำนาจตามตามกฎหมายกฎหมายจริง จริง</p> <p>หรือมีข้อยกเว้นตามกฎหมายประการอื่นที่ทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)</p>
5	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พิจารณาดำเนินการตามคำร้องขอ หรือไม่ <p>5.1 กรณีดำเนินการตามคำร้องขอ: แจ้งผู้ควบคุมข้อมูลส่วนบุคคลให้ดำเนินการ</p> <p>5.2 กรณีไม่ดำเนินการตามคำร้องขอ: แจ้งปฏิเสธผู้ร้องขอ พร้อมเหตุผลการปฏิเสธ</p>
6	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดำเนินการเก็บบันทึกแบบคำร้องขอ และบันทึกรายละเอียดสำหรับเจ้าหน้าที่ ในแบบคำร้องขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ

6. คู่มือปฏิบัติงานกรณีเกิดข้อร้องเรียน

การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล

6.1 วัตถุประสงค์

คู่มือปฏิบัติงานกรณีเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล จัดทำขึ้น เพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานในกรณีการเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคล และการรั่วไหลข้อมูลส่วนบุคคล เพื่อป้องกันหรือระงับเหตุการณ์การละเมิด และการรั่วไหลข้อมูล

6.2 ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

1. ผู้พบเหตุการณ์ มีหน้าที่ความรับผิดชอบในการแจ้ง DPO

เมื่อพบเห็นเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล

2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ความรับผิดชอบ ดังนี้

- 1) บันทึกเหตุการณ์ และแจ้งผู้ที่เกี่ยวข้อง เพื่อดำเนินการแก้ปัญหา
- 2) ประเมินความเสี่ยงร่วมกับบุคคลที่เกี่ยวข้อง
- 3) ดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล
- 4) ดำเนินการแจ้งต่อสำนักงาน

6.3 ขั้นตอนปฏิบัติงานต่อการแจ้งเหตุละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล

ขั้นตอนที่	รายละเอียด
1	ผู้พบเห็นเหตุการณ์ พบเห็นเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล ให้ดำเนินการแจ้ง DPO เพื่อทราบ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป ตามแบบคำร้องการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล ศคธ.
2	DPO บันทึกเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล ศคธ. และแจ้งบุคคลที่เกี่ยวข้องเพื่อดำเนินการแก้ไขต่อไป
3	DPO ประเมินความเสี่ยงของเหตุการณ์การละเมิดข้อมูลหรือการรั่วไหลส่วนบุคคลร่วมกับผู้ที่เกี่ยวข้องที่ได้รับไว้ในข้อ 6.5 เกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล และบันทึกในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล ศคธ.
4	DPO ดำเนินการตรวจสอบเกณฑ์ที่จะต้องแจ้งสำนักงาน และ/หรือ เจ้าของข้อมูลส่วนบุคคล ในข้อ 6.5 เกณฑ์การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล และดำเนินการดังนี้ 4.1 กรณีแจ้งแก่สำนักงาน: 4.1.1 DPO แจ้งเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลมายังฝ่ายดิจิทัล 4.1.2 DPO แจ้งเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล แก่สำนักงานเพื่อทราบโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุการณ์ หรือเท่าที่จะสามารถกระทำได้ โดยใช้หนังสือแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach

	Notification) แจ้งผ่านทางอีเมล pdpc@mdes.go.th หรือช่องทางอื่นที่สามารถแจ้ง แก่สำนักงานได้ 4.2 กรณีแจ้งแก่เจ้าของข้อมูลส่วนบุคคล: DPO ประเมินผลกระทบแก่เจ้าของข้อมูลส่วนบุคคล และแจ้งเหตุการณ์การละเมิดหรือการรั่วไหล ผลกระทบที่เกิดขึ้น และมาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า
5	DPO บันทึกการดำเนินการ และผลกระทบเหตุการณ์การละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลที่เกิดขึ้นในแบบบันทึกการละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคล
6	DPO ร่วมกับฝ่ายงานที่เกี่ยวข้อง ทบทวนมาตรการความปลอดภัยข้อมูลส่วนบุคคล โดยใช้ปัจจัยพิจารณาจากข้อ 6.5 ปัจจัยที่ต้องพิจารณาเพื่อการประเมินความเสี่ยงของข้อมูลส่วนบุคคล และดำเนินการ ดังนี้ 6.1 กรณีเกิดเหตุจากเอกสารจัดเก็บ: DPO ร่วมกับเจ้าของข้อมูลส่วนบุคคลในหน่วยงาน ทบทวน และออกมาตรการการรักษาความปลอดภัยเพิ่มเติม หากมีความจำเป็น 6.2 กรณีเกิดเหตุทางช่องทางอิเล็กทรอนิกส์: DPO ร่วมกับฝ่ายดิจิทัล ทบทวน และแนวทางปรับปรุงนโยบายความมั่นคงปลอดภัยของข้อมูล ให้เป็นปัจจุบันหากมีความจำเป็นต้องเสริมมาตรการเพิ่มเติม

6.4 ช่องทางติดต่อ DPO

หากมีข้อสงสัย ข้อเสนอแนะ หรือข้อกังวลเกี่ยวกับเกี่ยวกับคู่มือปฏิบัติงานกรณีเกิดข้อร้องเรียน การละเมิดข้อมูลส่วนบุคคลหรือการรั่วไหลของข้อมูลส่วนบุคคล หรือต้องการแจ้งเหตุการณ์การละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล สามารถติดต่อสอบถามได้ที่

- 1) ติดต่อด้วยตนเอง ณ ศูนย์คุณธรรม (องค์การมหาชน) ชั้น 16-17 อาคารวิทยาลัยการจัดการ มหาวิทยาลัยมหิดล แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400 เวลาทำการ (08:30 – 16:30 น.) วันจันทร์ - วันศุกร์ (ยกเว้นวันหยุดที่ราชการกำหนด)
- 2) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail): info@moralcenter.or.th
- 3) โทรศัพท์: 0 2644 9900

6.5 การประเมินระดับผลกระทบที่มีต่อเจ้าของข้อมูลส่วนบุคคล

เพื่อใช้ประเมินระดับผลกระทบเมื่อเกิดเหตุการณ์การละเมิดข้อมูลส่วนบุคคล

โดยตรวจสอบว่าเข้าเกณฑ์ที่จะต้องแจ้งสำนักงาน และ/หรือ เจ้าของข้อมูลส่วนบุคคลหรือไม่ (อ้างอิงจากข้อ 7 - 9 ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566)

1. พิจารณาประเภทผลกระทบที่อาจเกิดขึ้น (มูลค่าความเสียหาย, จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ, ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน, ความมั่นคงของรัฐและความสงบเรียบร้อย)
2. ประเมินระดับผลกระทบการละเมิด (ระดับต่ำ กลาง สูง)
3. ประเมินระดับความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล (ไม่เสี่ยงต่อสิทธิเสรีภาพ, เสี่ยง, เสี่ยงสูง)
4. ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไขฟื้นฟู และทบทวนมาตรการความปลอดภัย

7. แนวทางปฏิบัติการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

7.1 วัตถุประสงค์

แนวทางปฏิบัติการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจัดทำขึ้น

เพื่อให้ผู้เกี่ยวข้องใช้เป็นคู่มือในการปฏิบัติงานเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ซึ่ง ค.ค.ร.

อาจมีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

เพื่อดำเนินการตามวัตถุประสงค์ในการให้บริการ เช่น เพื่อส่งต่อข้อมูลส่วนบุคคลไปยังระบบคลาวด์ (Cloud)

ที่มีแพลตฟอร์มหรือเซิร์ฟเวอร์ (Server) อยู่ต่างประเทศ

โดยจะทำให้แน่ใจว่าประเทศปลายทางมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามมาตรฐานสากลหรือดำเนินการตามเงื่อนไข เพื่อให้สามารถส่งหรือโอนข้อมูลนั้นได้ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

7.2 ผู้รับผิดชอบและหน้าที่ความรับผิดชอบ

ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ความรับผิดชอบตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

7.3 ขั้นตอนปฏิบัติงานต่อการโอนข้อมูลไปยังต่างประเทศ

7.3.1 ผู้ควบคุมข้อมูลส่วนบุคคล พิจารณาการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

หรือองค์การระหว่างประเทศ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือไม่

- กรณีไม่เป็นการส่งข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ สามารถดำเนินการ โดยไม่ต้องปฏิบัติตามหลักเกณฑ์และเงื่อนไขที่กำหนดในมาตรา 28 และมาตรา 29 ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีรายละเอียดตาม ข้อ 5 มาตราที่เกี่ยวข้อง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- กรณีที่ตกอยู่ในข้อบังคับของกฎหมาย ให้ดำเนินการตามข้อ 7.3.2 ต่อไป

7.3.2 ผู้ควบคุมข้อมูลส่วนบุคคล ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ให้ดำเนินการดังนี้

7.3.2.1

กรณีประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่ เพียงพอ หรือไม่

กรณีมีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคล สามารถโอนข้อมูลส่วนบุคคลได้

กรณีไม่ปรากฏว่ามีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ผู้ควบคุมข้อมูลส่วนบุคคล

ไม่สามารถส่งหรือโอนข้อมูลส่วนบุคคลได้ และให้ดำเนินการตาม 7.3.3 ต่อไป

7.3.2.2 กรณีได้รับการยกเว้นตามกฎหมายให้ส่งหรือโอนได้ แม้ว่าประเทศปลายทางหรือ

องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคล

กรณีอยู่ในข้อยกเว้นตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคล

สามารถโอนข้อมูลส่วนบุคคลได้แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลไม่มีมา ตรฐาน คุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยพิจารณาข้อยกเว้นตามกฎหมาย ดังนี้

1) เป็นการปฏิบัติตามกฎหมาย

2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูล

ส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การ ระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา

หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือ นิติบุคคลอื่น

เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล ส่วนบุคคลหรือบุคคลอื่น

เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

- กรณีไม่สามารถปรับใช้ข้อยกเว้นตามกฎหมายได้ ผู้ควบคุมข้อมูลส่วนบุคคล

ไม่สามารถส่งหรือโอนข้อมูลส่วนบุคคลได้ และให้ดำเนินการตาม 7.3.3 ต่อไป

7.3.3 ศคช. มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคล

เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือไม่

กรณีมีนโยบายในการคุ้มครองข้อมูลส่วนบุคคล เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับ

การตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล

สามารถโอนข้อมูลส่วนบุคคลได้

แม้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะไม่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

กรณีไม่ปรากฏนโยบายดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคล

ไม่สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลได้

7.4 มาตรการที่เกี่ยวกับการส่งหรือโอนข้อมูลไปยังต่างประเทศ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูล

ส่วนบุคคลที่เพียงพอ ทั้งนี้

ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา

16 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคล

ทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่าง

ประเทศที่รับข้อมูลส่วนบุคคลแล้ว

- (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- (4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นเมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- (6) เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะที่สำคัญ ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทาง หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
- มาตรา 29 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองดังกล่าวให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28
- นโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรวจสอบและรับรองตามวรรคหนึ่งให้เป็นไปตามที่คณะกรรมการประกาศกำหนด
- ในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการตามมาตรา 28 หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28 เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสม

สามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

8. แนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคล (Data Retention and Disposal Policy)

8.1 วัตถุประสงค์

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็นแนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดการเก็บรักษาและไม่มีให้นำข้อมูลกลับมาประมวลผล หรือเมื่อเจ้าของข้อมูลมีการร้องขอให้ทำลายข้อมูล

8.2 ประเภทของข้อมูลส่วนบุคคลที่ ศคธ. เก็บรวบรวม

ในการเก็บรวบรวม และเก็บรักษาข้อมูลส่วนบุคคล ศคธ.

จะใช้วิธีการที่ชอบด้วยกฎหมายและจำกัดเพียงเท่าที่จำเป็นตามวัตถุประสงค์การดำเนินงานของ ศคธ.

อันประกอบด้วย

ประเภทข้อมูลส่วนบุคคล	รายละเอียดและตัวอย่าง
ข้อมูลเฉพาะตัวบุคคล	ข้อมูลระบุชื่อเรียกของบุคคลหรือข้อมูลจากที่ระบุข้อมูลเฉพาะตัวของบุคคล เช่น ชื่อ-นามสกุล อายุ วันเดือนปีเกิด เพศ สัญชาติ อาชีพ หมายเลขบัตรประจำตัวประชาชนหรือหมายเลขหนังสือเดินทาง ประสบการณ์ทำงาน ประวัติการเรียนรู้ การศึกษา ตำแหน่ง เป็นต้น ที่สามารถระบุตัวตนได้
ข้อมูลสำหรับการติดต่อ	ข้อมูลสำหรับการติดต่อบุคคล เช่น ที่อยู่ หมายเลขโทรศัพท์ อีเมล ชื่อ บัญชี Social Media สถานที่ทำงาน เป็นต้น
ข้อมูลเอกสารทางราชการ	ข้อมูลเอกสารราชการของบุคคล เช่น สำเนาบัตรประชาชน สำเนา ทะเบียนบ้าน สำเนาหนังสือเดินทาง สำเนาสูติบัตร สำเนาใบอนุญาตเข้าทำงาน สำเนาใบอนุญาตขับขี่ สำเนาใบประกอบวิชาชีพ เป็นต้น
ข้อมูลทางการเงิน	ข้อมูลทางการเงินของบุคคล เช่น เลขบัญชีเงินธนาคาร สำเนาหน้าบัญชีธนาคาร เลขบัตรเครดิต รายได้ เงินเดือน การค้าประกัน ข้อมูลวงเงิน เครดิต ข้อมูลการทำธุรกรรม วิธีการชำระเงิน การจ่ายภาษี กองทุนสำรองเลี้ยงชีพ ผลประโยชน์ของพนักงาน (สิทธิตามกรมธรรม์ประกันภัย) รวมถึงข้อมูลอื่น ๆ ที่เกี่ยวข้อง (เบี้ยเลี้ยง) เป็นต้น
ข้อมูลที่ได้จากเก็บรวบรวมของ ศคธ. หรือระบบอัตโนมัติจากอุปกรณ์ต่าง ๆ ของ ศคธ.	ข้อมูลที่ได้จากเก็บรวบรวมของ ศคธ. หรือระบบอัตโนมัติจากอุปกรณ์ต่างของ ศคธ. เช่น ภาพจากกล้องวงจรปิด ภาพถ่าย ภาพเคลื่อนไหว เสียงบันทึกการสนทนา เป็นต้น
ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนของท่าน เช่น เชื้อชาติ ข้อมูล ศาสนา ข้อมูลความพิการ ประวัติอาชญากรรม ข้อมูลชีวภาพ (ข้อมูลจำลองลายนิ้วมือ ข้อมูลภาพจำลองใบหน้า) ข้อมูลเกี่ยวกับสุขภาพ เป็นต้น หรือข้อมูลอื่นใดในทำนองเดียวกันที่กฎหมายกำหนด
ข้อมูลของบุคคลที่สาม ข้อมูลอื่น	ข้อมูลสมาชิกในครอบครัว ข้อมูลผู้รับประโยชน์จากสวัสดิการต่าง ๆ ข้อมูลผู้ติดต่อฉุกเฉิน

ๆ	ข้อมูลผู้ค้าประกันการทำงาน และบุคคลอ้างอิง การใช้งานเว็บไซต์ ความคิดเห็น ความชื่นชอบ เสียข นวัตกรรม ภาพนิ่ง ภาพเคลื่อนไหว รวมถึงการเข้าร่วมกิจกรรม หรือแคมเปญต่าง ๆ ที่ ศคธ. จัดขึ้น และข้อมูลอื่นใดที่ถือว่าเป็นข้อมูลส่วนบุคคลตามกฎหมาย
ระยะเวลาการเก็บรักษา	ช่วงเวลาที่เหมาะสมที่พิจารณาเห็นสมควรให้มีการเก็บรักษาข้อมูลส่วนบุคคลเหล่านั้นไว้เพื่อประโยชน์ในการประมวลผลข้อมูลส่วนบุคคล ซึ่งต้องสอดคล้องตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลส่วนบุคคล โดยจะจัดเก็บไว้เป็นระยะเวลาหนึ่งตามความจำเป็นเท่านั้น
การลบทำลายข้อมูล (Data Deletion and Destruction)	การทำให้ข้อมูลส่วนบุคคลไม่สามารถบ่งชี้กลับมายังตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้อีก โดยอาศัยวิธีการลบทำลายต่างๆ ที่เหมาะสมตามชนิดหรือรูปแบบของการจัดเก็บข้อมูล

8.3 การกำหนดระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 วรรค 3

ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ดังนั้น ศคธ.

จึงกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละประเภท ดังนี้

ประเภทของข้อมูล	สื่อที่ใช้เก็บข้อมูล	ระยะเวลาในการเก็บรักษาข้อมูล
ข้อมูลส่วนบุคคลของเจ้าหน้าที่หรือผู้ปฏิบัติงาน ลูกจ้าง	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของผู้ปฏิบัติงาน (PC, Notebook)	10 ปีหลังสิ้นสุดสภาพการเป็นพนักงาน
ระบบสแกนลายนิ้วมือ/หน้า	ฐานข้อมูลระบบ Time Attendance กระดาษ (Paper)	ไม่เกิน 1 ปีหลังสิ้นสุดสภาพการเป็นพนักงาน (โดยสามารถดูข้อมูลย้อนหลังได้ภายใน 1 ปี) สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้ใช้บริการหรือผู้รับบริการด้านอื่นๆ ที่มาขอใช้บริการจาก ศคธ.	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	ไม่เกิน 1 ปี หรือหลังจากใช้บริการไม่มีสิทธิและหน้าที่ใด ๆ กับ บริษัทฯ สอดคล้องตามกฎหมายระเบียบข้อบังคับ และ แนวปฏิบัติที่เกี่ยวข้อง และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของ กรรมการ ผู้รับมอบอำนาจ ผู้แทน ตัวแทน ผู้ถือหุ้น ลูกจ้าง หรือบุคคลอื่นที่มีความสัมพันธ์ในรูปแบบเดียวกัน	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ	ไม่เกิน 1 ปี หรือหลังจากใช้บริการ ไม่มีสิทธิและหน้าที่ใด ๆ กับ บริษัทฯ สอดคล้องตาม กฎหมายระเบียบข้อบังคับ และ แนวปฏิบัติที่เกี่ยวข้อง สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง

องนิตบุคคลที่มีความสัมพันธ์กับ ศคธ.	ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้เข้าร่วมประชุม อบรม สัมมนา หรือกิจกรรมที่เป็นข้อมูลส่วนบุคคลที่ ทั่วไป	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	ภายหลังจากผู้ให้บริการ ไม่มีสิทธิและหน้าที่ใด ๆ กับบริษัทฯ สอดคล้องตามกฎหมายระเบียบ ข้อบังคับ และ แนวปฏิบัติที่เกี่ยวข้อง สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้เข้าร่วมประชุม อบรม สัมมนา หรือกิจกรรมที่เป็นข้อมูลส่วนบุคคลที่ มีความอ่อนไหว	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	ทันทีหลังจากผู้ให้บริการ ไม่มีสิทธิและหน้าที่ใด ๆ กับบริษัทฯ สอดคล้องตามกฎหมายระเบียบ ข้อบังคับ และ แนวปฏิบัติที่เกี่ยวข้อง สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลที่เป็นหลักฐานการจั ตซื้อจัดจ้าง	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	สอดคล้องตามกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ และกฎหมายว่าด้วยงานสารบรรณ สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้สมัครงาน	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	ไม่เกิน 1 ปี สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้สมัครงานที่ฝ่า นการคัดเลือกและขึ้นบัญชีไว้	ฐานข้อมูล (Database) ระบบจัดเก็บข้อมูล (File Server) เครื่องคอมพิวเตอร์ของ ผู้ปฏิบัติงาน (PC, Notebook) กระดาษ (Paper)	ไม่เกิน 2 ปี สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ และกฎหมายระเบียบข้อบังคับและแนวปฏิบัติที่เกี่ยวข้อง หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
ข้อมูลส่วนบุคคลของผู้มาติดต่อ	สมุดบันทึกการแลกบัตร เพื่อเข้า-ออก	ไม่เกิน 1 ปี

	สถานที่ปฏิบัติงาน หรือสถานที่สำคัญของบริษัทฯ	
ข้อมูลส่วนบุคคลจากกล้อง CCTV	ระบบ CCTV	30 วัน หรือเท่าที่จำเป็นในการปฏิบัติงาน
ข้อมูลส่วนบุคคลของผู้เข้าชมหรือใช้งานเว็บไซต์ https://www.moralcenter.or.th รวมทั้งระบบ แอปพลิเคชัน อุปกรณ์ หรือช่องทางการสื่อสารอื่นซึ่งควบคุมดูแลโดย ศศร.	เครื่องให้บริการของระบบ ต่าง ๆ ระบบจัดเก็บข้อมูล Log ระบบ WIFI Controller	90 วัน หรือเท่าที่จำเป็นในการปฏิบัติงาน
ข้อมูลบัญชีผู้ใช้งานบนระบบอิเล็กทรอนิกส์ต่าง ๆ ของบริษัทฯ	ระบบพิสูจน์และยืนยันตัวตน (Active Directory)	เมื่อผู้ใช้งานขอให้ยกเลิกการใช้งานหรือเมื่อมีการยกเลิกการใช้งานระบบอิเล็กทรอนิกส์นั้น ๆ อย่างเป็นทางการ
ข้อมูลส่วนบุคคลที่ใช้ติดต่อประสานงานบนระบบอีเมล	ระบบอีเมล	สอดคล้องตามกฎหมายว่าด้วยงานสารบรรณ หรือตามสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กำหนด
ข้อมูลการให้ความยินยอม	ระบบ Privacy Notice and Consent Management	ตลอดระยะเวลาดำเนินงานของกิจกรรมที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล

8.4 การทำข้อมูลนิรนาม (Anonymization)

แนวทางในการทำลายข้อมูลส่วนบุคคลแบ่งออกเป็น 2 วิธีดังนี้

1. ทำลายสื่อที่ใช้เก็บบันทึกข้อมูลส่วนบุคคล
2. การจัดทำข้อมูลส่วนบุคคลให้เป็นข้อมูลนิรนาม (Anonymization)

การจัดทำข้อมูลนิรนาม คือ กระบวนการที่ทำให้ความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลนั้นน้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (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 วิธีดังกล่าวนี้ทวีความนิยมมากขึ้นในภาครัฐภาคเอกชนทั่วโลก เช่น มีชุดข้อมูลเป็น สีรถและทะเบียนรถ อาจลดข้อมูลเหลือ สีรถ

- Pseudonymization การแฝงข้อมูล เป็นวิธีการในการแทนที่สิ่งที่ระบุตัวตนของเจ้าของข้อมูลโดยตรงเช่น ชื่อ ที่อยู่ หรือ รหัสประจำตัวต่าง ๆ ด้วยชื่อหรือรหัสที่สร้างขึ้นมา

- De-identification การขจัดตัวตน คือ การลบข้อมูลในส่วนที่จะทำให้มีการระบุตัวตนใหม่

เป็นการป้องกันการย้อนรอยเพื่อระบุตัวตน (re-identification) โดยพิจารณาถึงตัวข้อมูลเป็นหลัก

ซึ่งหมายรวมถึงการแฝงข้อมูลด้วย เช่น มีชุดข้อมูล ชื่อ นายเด๊ด อีเมล dad@moralcenter.or.th เบอร์โทร 0987654321 แสดงเป็น นาย A อีเมล - เบอร์โทร -

8.5 การลบทำลายข้อมูลส่วนบุคคล

8.5.1. ขั้นตอนการลบทำลายข้อมูลส่วนบุคคล

1. หลักเกณฑ์ในการเริ่มต้นกระบวนการ

- เมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้มีการทำลายข้อมูลส่วนบุคคล

2. ขั้นตอนการปฏิบัติงาน

2.1 คณะทำงานคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

ขออนุญาตทำลายข้อมูลส่วนบุคคลที่ครบกำหนดหรือเจ้าของข้อมูลส่วนบุคคลมีการร้องขอให้ทำลายอย่างเป็นลายลักษณ์อักษร พร้อมทั้งระบุเหตุผลการทำลาย และวิธีการที่จะใช้ในการทำลายข้อมูลส่วนบุคคล

2.2 ผู้บริหารหน่วยงาน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการพิจารณา และอนุมัติในการทำลายข้อมูล

- กรณีให้ทำลาย ให้ดำเนินการต่อในข้อ 2.3
- กรณีที่ไม่ให้ทำลายให้สิ้นสุดกระบวนการ

2.3 คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) ดำเนินการทำลายข้อมูลส่วนบุคคลตามแนวทางในการทำลายข้อมูลส่วนบุคคล

2.4 คณะทำงานข้อมูลส่วนบุคคล (ถ้ามี) บันทึกหลักฐานการทำลายข้อมูลส่วนบุคคล

8.5.2 วิธีการลบทำลายข้อมูลส่วนบุคคล

ที่	ประเภทสื่อที่ใช้เก็บ	การลบทำลายข้อมูล
1	บนกระดาษ	ทำลายด้วยเครื่องทำลายเอกสาร ที่ไม่สามารถนำซากเอกสารที่ทำลายแล้วมาประกอบและอ่านข้อมูลได้ หรือตามกฎหมายว่าด้วยงานสารบรรณกำหนด <ul style="list-style-type: none"> เผาทำลาย
2	ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ	ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ศคธ. กำหนดให้ใช้งาน รวมถึง ต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูล การลบชั่วคราว (Recycle Bin) เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนาม ซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
3	บนเครื่องให้บริการ หรือฐานข้อมูลของระบบสารสนเทศต่างๆ	ใช้คำสั่งการลบทำลาย (delete) ของระบบบริหารจัดการฐานข้อมูล ใช้คำสั่งการลบทำลาย (delete) เครื่องให้บริการระบบ (Virtual Machine) ที่ควบคุมการเข้าถึงข้อมูลนั้น ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
4	บนสื่อบันทึกข้อมูลประเภทฮาร์ดดิสก์	ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลบริษัทฯ กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูล การลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ อาทิ Hard disk ประเภทจานหมุน ทำให้แผ่นเก็บข้อมูลภายในเป็นรอยขีด ข่วน ร้ายแรง (ทุบ เจาะ บดขยี้) หรือ ใช้เครื่องทำลายแบบ Degaussing หรือ De-identification Hard disk ประเภท SSD ถอดแยกชิ้นส่วน และทำลายแผงวงจร ภายในจนไม่สามารถประกอบใช้งานได้ (ทุบ เจาะ บดขยี้) หรือ ใช้ เครื่องทำลายแบบ Degaussing หรือ De-identification ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
5	บนสื่อบันทึกข้อมูลประเภทเคลื่อนที่ได้	ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลบริษัทฯ กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูล การลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ อาทิ ใช้เครื่องทำลาย CD/DVD หรือหักทำลายเป็นส่วน ๆ อย่างน้อย 4 ส่วน Thumb drive ถอดแยกชิ้นส่วน และทำลายแผงวงจร ภายในจนไม่สามารถประกอบใช้งานได้ หรือ De-identification ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนาม ซึ่งไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
6	บนคลาวด์	ใช้คำสั่งการลบทำลาย (delete) หรือซอฟต์แวร์ลบทำลายข้อมูลที่ ศคธ. กำหนดให้ใช้งาน รวมถึงต้องตามไปดำเนินการลบในแหล่งที่จัดเก็บข้อมูล การลบชั่วคราว เพื่อป้องกันการกู้คืนกลับมาได้ใหม่ ใช้คำสั่งการลบทำลาย (delete) เครื่องให้บริการระบบ (Virtual Machine)

	<p>ที่ควบคุมการเข้าถึงข้อมูลนั้น (ในกรณีที่เป็นการให้บริการ คลาวด์ที่อนุญาตให้มีการสร้างเครื่องให้บริการได้ และไม่มีการใช้งาน เครื่องให้บริการนั้นอีกต่อไป) ใช้มาตรการเชิงเทคนิคเพื่อทำให้เป็นข้อมูลนิรนามซึ่งไม่สามารถระบุตัว บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้</p>
--	--

อ้างอิง ประกาศบริษัทฯ เรื่อง นโยบายและแนวปฏิบัติการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management) ข้อ 5. การทำลายข้อมูล ประกาศ ณ วันที่ 19 ธันวาคม 256X

8.5.3 การจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล

การจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล

กรณีที่มีการจ้างผู้ให้บริการภายนอกในการทำลายข้อมูลส่วนบุคคล ต้องมีการกำกับ และควบคุมกระบวนการระหว่างการทำลาย และเก็บรวบรวมหลักฐานการทำลายข้อมูลส่วนบุคคลจากผู้ให้บริการภายนอก และดำเนินการตามกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ

ศูนย์คุณธรรม (องค์การมหาชน)