ราชวิทยาลัย
จุฬาภรณ์

ประกาศราชวิทยาลัยจุฬาภรณ์
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๖๙

.....

โดยที่ราชวิทยาลัยจุฬาภรณ์เป็นสถาบันการศึกษาวิจัยด้านวิทยาศาสตร์สุขภาพและเป็นหน่วยบริการทางการแพทย์และสาธารณสุข มีพันธกิจด้านการจัดการศึกษาเพื่อสร้างบัณฑิตและนักวิจัย การวิจัยและสร้างนวัตกรรม การให้บริการทางการแพทย์และสาธารณสุขอย่างเป็นธรรม การบริหารจัดการองค์กร การสืบสานศิลปวัฒนธรรมและศาสนา และการสืบสานพระปณิธานในการช่วยเหลือประชาชน การดำเนินพันธกิจดังกล่าวจำเป็นต้องมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้ป่วยและผู้รับบริการ นักศึกษาและผู้เข้ารับการฝึกอบรม ผู้สมัครงาน ผู้ปฏิบัติงานและบุคคลในครอบครัว อาสาสมัครและผู้เข้าร่วมโครงการวิจัย ตลอดจนบุคคลอื่นที่เกี่ยวข้อง ซึ่งส่วนหนึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยเฉพาะข้อมูลสุขภาพ

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัยจุฬาภรณ์เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และกฎหมายอื่นที่เกี่ยวข้อง เป็นไปในแนวทางเดียวกันทุกส่วนงาน และมีมาตรฐานสอดคล้องกับระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่ราชวิทยาลัยจุฬาภรณ์ได้รับการรับรอง จึงสมควรกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นหลักปฏิบัติ

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติราชวิทยาลัยจุฬาภรณ์ พ.ศ.๒๕๕๙ และที่แก้ไขเพิ่มเติม และคำสั่งราชวิทยาลัยจุฬาภรณ์ ที่ พิเศษ ๔/๒๕๖๗ เรื่อง มอบอำนาจการดำเนินงานของราชวิทยาลัยจุฬาภรณ์ ลงวันที่ ๒๖ ธันวาคม พ.ศ. ๒๕๖๗ ประกอบมติที่ประชุมคณะกรรมการบริหารราชวิทยาลัยจุฬาภรณ์ ในการประชุมครั้งที่ ๑๙/๒๕๖๙ เมื่อวันที่ ๖ ตุลาคม พ.ศ.๒๕๖๙ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศราชวิทยาลัยจุฬาภรณ์ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกประกาศราชวิทยาลัยจุฬาภรณ์ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัยจุฬาภรณ์ ประกาศ ณ วันที่ ๘ พฤษภาคม พ.ศ.๒๕๖๓

บรรดาประกาศ คำสั่ง หลักเกณฑ์ และแนวปฏิบัติอื่นใดที่ขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔ ในประกาศนี้

"ราชวิทยาลัย" หมายความว่า ราชวิทยาลัยจุฬาภรณ์

"ส่วนงาน" หมายความว่า ส่วนงานของราชวิทยาลัยตามมาตรา ๘ แห่งพระราชบัญญัติราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๕๙ และให้หมายความรวมถึงส่วนงานที่ราชวิทยาลัยตั้งขึ้นที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าส่วนงาน และได้รับอนุมัติจากสภาราชวิทยาลัยจุฬาภรณ์

"หน่วยงาน" หมายความว่า หน่วยงานภายในของส่วนงาน

"ผู้ปฏิบัติงานในราชวิทยาลัย" หมายความว่า พนักงานและลูกจ้างของราชวิทยาลัย

"ผู้ใช้ข้อมูลส่วนบุคคล" หมายความว่า ผู้บังคับบัญชา หัวหน้าส่วนงาน หัวหน้าหน่วยงาน ผู้ปฏิบัติงานในราชวิทยาลัย ผู้ประกอบวิชาชีพด้านสุขภาพ อาจารย์ นักศึกษา ผู้เข้ารับการฝึกอบรม แพทย์ประจำบ้าน ผู้ปฏิบัติงานภายใต้การกำกับดูแลของราชวิทยาลัย ผู้รับจ้าง ที่ปรึกษา ผู้ประมวลผลข้อมูลส่วนบุคคล และบุคคลภายนอกซึ่งได้รับสิทธิให้เข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของราชวิทยาลัย ได้ทำการเข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของราชวิทยาลัย

"คณะกรรมการบริหาร" หมายความว่า คณะกรรมการบริหารราชวิทยาลัยจุฬาภรณ์ตามมาตรา ๒๕ แห่งพระราชบัญญัติราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๕๙

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ข้อมูลอ่อนไหว" หมายความว่า ข้อมูลส่วนบุคคลตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเฉพาะอย่างยิ่งข้อมูลสุขภาพ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ และข้อมูลความพิการ

"เจ้าของข้อมูลส่วนบุคคล" หมายความว่า บุคคลธรรมดาซึ่งข้อมูลส่วนบุคคลนั้นระบุถึง และให้หมายความรวมถึงผู้ใช้อำนาจปกครอง ผู้อนุบาล หรือผู้พิทักษ์ ซึ่งมีอำนาจกระทำการแทนตามกฎหมาย

"การประมวลผล" หมายความว่า การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล รวมถึงการเก็บรวบรวม ใช้ เปิดเผย บันทึก จัดเก็บ เปลี่ยนแปลง แก้ไข ส่ง โอน เผยแพร่ ลบ หรือทำลาย

"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" หรือ "DPO" หมายความว่า เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลซึ่งราชวิทยาลัยแต่งตั้งตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

"เหตุการละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดความลับ ความถูกต้องครบถ้วน หรือความพร้อมใช้งานของข้อมูลส่วนบุคคล ไม่ว่าจะเกิดจากการกระทำโดยปราศจากอำนาจหรือโดยมิชอบ ความประมาทเลินเล่อ อุบัติเหตุ หรือเหตุอื่นใด

ข้อ ๕ ให้เลขาธิการราชวิทยาลัยจุฬาภรณ์เป็นผู้รักษาการตามประกาศนี้ และมีอำนาจออกประกาศหรือคำสั่งเพื่อปฏิบัติให้เป็นไปตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติหรือไม่สามารถปฏิบัติตามประกาศนี้ ให้เลขาธิการราชวิทยาลัยจุฬาภรณ์เป็นผู้วินิจฉัยชี้ขาดและถือเป็นที่สุด

หมวด ๑
บททั่วไป

.....

ข้อ ๖ ขอบเขตการบังคับใช้ ประกาศนี้ใช้บังคับกับทุกส่วนงานและหน่วยงานภายในของส่วนงาน และใช้บังคับกับการดำเนินกิจกรรมทุกประเภทตามพันธกิจของราชวิทยาลัยที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะกระทำด้วยระบบสารสนเทศหรือด้วยเอกสาร

ประกาศนี้ให้ใช้บังคับกับบุคคลดังต่อไปนี้ด้วย

(๑) ผู้บังคับบัญชา หัวหน้าส่วนงาน หัวหน้าหน่วยงาน และผู้ปฏิบัติงานในราชวิทยาลัยทุกคน

(๒) ผู้ประกอบวิชาชีพด้านสุขภาพ อาจารย์ นักศึกษา ผู้เข้ารับการฝึกอบรม แพทย์ประจำบ้าน และผู้ปฏิบัติงานภายใต้การกำกับดูแลของราชวิทยาลัย

(๓) ผู้รับจ้าง ที่ปรึกษา ผู้ประมวลผลข้อมูลส่วนบุคคล และบุคคลภายนอกซึ่งได้รับสิทธิให้เข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของราชวิทยาลัย

ข้อ ๗ หลักการคุ้มครองข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลของราชวิทยาลัยต้องเป็นไปตามหลักการดังต่อไปนี้

(๑) หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness, Fairness and Transparency) โดยต้องมีฐานทางกฎหมายรองรับ และแจ้งวัตถุประสงค์ ข้อมูลส่วนบุคคลที่เก็บรวบรวม และระยะเวลาเก็บรักษา

(๒) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation) โดยประมวลผลตามวัตถุประสงค์ที่กำหนดและได้แจ้งไว้แล้วเท่านั้น การประมวลผลที่แตกต่างไปจากวัตถุประสงค์เดิมจะกระทำมิได้ เว้นแต่ได้แจ้งวัตถุประสงค์ใหม่และมีฐานทางกฎหมายรองรับ

(๓) หลักการเก็บรวบรวมข้อมูลส่วนบุคคลให้น้อยที่สุดเท่าที่จำเป็น (Data Minimization) โดยต้องไม่ขอหรือใช้ข้อมูลเกินความจำเป็นแก่วัตถุประสงค์

(๔) หลักความถูกต้องครบถ้วน (Accuracy) โดยต้องดูแลให้ข้อมูลส่วนบุคคลถูกต้องเป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด

(๕) หลักการเก็บรักษาข้อมูลส่วนบุคคลอย่างจำกัดระยะเวลา (Storage Limitation) โดยลบหรือทำลายเมื่อพ้นระยะเวลาหรือเกินความจำเป็น

(๖) หลักการรักษาความถูกต้องครบถ้วนและการรักษาความลับของข้อมูลส่วนบุคคล (Integrity and Confidentiality) โดยจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

(๗) หลักความรับผิดชอบ (Accountability) โดยต้องสามารถแสดงหลักฐานการปฏิบัติตามกฎหมายและประกาศนี้ได้

หมวด ๒
การกำกับดูแลและหน้าที่ความรับผิดชอบ

.....

ข้อ ๘ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัย ซึ่งคณะกรรมการบริหารเป็นผู้แต่งตั้ง เพื่อทำหน้าที่กำหนดทิศทาง พิจารณาให้ความเห็นชอบแนวปฏิบัติและมาตรการที่เกี่ยวข้อง กำกับติดตามการปฏิบัติตามประกาศนี้ พิจารณาเรื่องร้องเรียนและเหตุการละเมิดข้อมูลส่วนบุคคลที่มีนัยสำคัญ และรายงานผลต่อคณะกรรมการบริหารอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๙ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่และอำนาจตามมาตรา ๔๒ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และให้มีหน้าที่ดังต่อไปนี้

(๑) ให้คำแนะนำแก่ส่วนงานและหน่วยงานเกี่ยวกับการปฏิบัติตามกฎหมายและประกาศนี้

(๒) ตรวจสอบการดำเนินงานของส่วนงานและหน่วยงาน รวมถึงการเรียกเอกสาร ข้อมูลและบันทึกที่เกี่ยวข้องเพื่อประกอบการตรวจสอบ

(๓) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเป็นผู้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลในนามของราชวิทยาลัย

(๔) พิจารณาและดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(๕) จัดให้มีการประเมินความเสี่ยง การอบรม และการสร้างความตระหนักแก่ผู้ใช้ข้อมูลส่วนบุคคล

(๖) รายงานตรงต่อผู้บริหารสูงสุดของราชวิทยาลัย

ราชวิทยาลัยจะมิให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาจ้างเพราะเหตุที่ปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและประกาศนี้

ข้อ ๑๐ ให้หัวหน้าส่วนงานเป็นผู้รับผิดชอบการคุ้มครองข้อมูลส่วนบุคคลภายในส่วนงานของตน และให้หัวหน้าหน่วยงานรับผิดชอบในส่วนของหน่วยงานภายใน โดยมีหน้าที่จัดให้มีการปฏิบัติตามประกาศนี้ จัดทำและทบทวนบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล กำหนดและทบทวนสิทธิการเข้าถึงข้อมูลของผู้ปฏิบัติงานในสังกัด กำกับให้ผู้ปฏิบัติงานเข้ารับการอบรมตามที่ราชวิทยาลัยกำหนด และรายงานเหตุการละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยทันที

ข้อ ๑๑ ให้ทุกส่วนงานจัดให้มีผู้ประสานงานคุ้มครองข้อมูลส่วนบุคคลประจำส่วนงาน โดยมอบหมายผู้ปฏิบัติงานภายในส่วนงานอย่างน้อยหนึ่งคนเป็นผู้ประสานงานคุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่ประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จัดเก็บเอกสารหลักฐานการปฏิบัติตามประกาศนี้ และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามหมวด ๖ ของประกาศนี้

ข้อ ๑๒ หน้าที่ของผู้ใช้ข้อมูลส่วนบุคคล มีดังต่อไปนี้

(๑) เข้าถึงและใช้ข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ตามตำแหน่งและสิทธิที่ได้รับมอบหมายเท่านั้น

(๒) ไม่เปิดเผยข้อมูลส่วนบุคคลที่ล่วงรู้จากการปฏิบัติหน้าที่แก่บุคคลอื่น ไม่ว่าภายในหรือภายนอกราชวิทยาลัย เว้นแต่มีฐานทางกฎหมายรองรับและได้รับอนุมัติตามขั้นตอนที่กำหนด

(๓) ไม่นำข้อมูลส่วนบุคคลไปใช้เพื่อประโยชน์ส่วนตนหรือประโยชน์ของบุคคลอื่น

(๔) ไม่นำข้อมูลส่วนบุคคลออกจากระบบหรือสถานที่ของราชวิทยาลัย ไม่ว่าด้วยวิธีการคัดลอก บันทึก ถ่ายภาพ บันทึกภาพหน้าจอ หรือวิธีการอื่นใด เว้นแต่ได้รับอนุมัติจากหัวหน้าส่วนงานและดำเนินการตามมาตรการที่กำหนด

(๕) ไม่ส่งหรือแบ่งปันข้อมูลส่วนบุคคลผ่านบัญชีส่วนตัวหรือช่องทางสื่อสารส่วนบุคคลที่ราชวิทยาลัยมิได้รับรอง

(๖) รักษาความลับของรหัสผ่านและสิ่งที่ใช้ยืนยันตัวตน และไม่ใช้สิทธิของผู้อื่นหรือให้ผู้อื่นใช้สิทธิของตน

(๗) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลหรือเหตุที่น่าสงสัยว่าจะเป็นการละเมิดโดยทันทีตามหมวด ๖ ของประกาศนี้

(๘) ลงนามรับทราบหน้าที่และข้อตกลงการรักษาความลับตามแบบที่ราชวิทยาลัยกำหนด

หน้าที่ของผู้ใช้ข้อมูลส่วนบุคคลตามที่กำหนดไว้ในประกาศนี้ให้มีผลต่อไปแม้พ้นจากตำแหน่งหรือสิ้นสุดสัญญาจ้างแล้ว

ข้อ ๑๓ ให้หน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศจัดให้มีมาตรการควบคุมการเข้าถึงระบบและข้อมูล การบริหารจัดการสิทธิผู้ใช้งาน การเข้ารหัสข้อมูล การสำรองข้อมูล การบันทึกและสอบทานการเข้าถึงข้อมูล และการตรวจสอบช่องโหว่ของระบบ โดยสอดคล้องกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และมาตรฐานการจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่ราชวิทยาลัยถือปฏิบัติตลอดจนกฎหมายที่เกี่ยวข้อง

ข้อ ๑๔ ให้หน่วยงานที่รับผิดชอบด้านทรัพยากรบุคคลจัดให้มีการลงนามรับทราบหน้าที่และข้อตกลงการรักษาความลับเมื่อแรกเข้าปฏิบัติงาน จัดให้ผู้ปฏิบัติงานเข้ารับการอบรมตามข้อ ๓๗ ดำเนินการระงับหรือเพิกถอนสิทธิการเข้าถึงข้อมูลเมื่อมีการโยกย้ายหรือพ้นจากหน้าที่โดยไม่ชักช้า

หมวด ๓
การประมวลผลข้อมูลส่วนบุคคล

.....

ข้อ ๑๕ ฐานในการประมวลผล การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไปต้องมีฐานทางกฎหมายรองรับตามมาตรา ๒๔ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมิให้ใช้ความยินยอมเป็นฐานการประมวลผลในกรณีที่มีฐานอื่นที่เหมาะสมกว่า โดยเฉพาะการประมวลผลข้อมูลของผู้ปฏิบัติงานในราชวิทยาลัยและผู้สมัครงานซึ่งมีความสัมพันธ์เชิงอำนาจระหว่างนายจ้างกับลูกจ้าง

ข้อ ๑๖ ข้อมูลอ่อนไหวและข้อมูลสุขภาพ การประมวลผลข้อมูลอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้นตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำหรับข้อมูลด้านสุขภาพของผู้ป่วย ให้ถือปฏิบัติตามมาตรา ๗ แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. ๒๕๕๐ และมาตรา ๓๒๓ แห่งประมวลกฎหมายอาญาประกอบด้วยโดยการเข้าถึงข้อมูลสุขภาพให้จำกัดเฉพาะผู้ปฏิบัติหน้าที่ที่เกี่ยวข้องกับการรักษาพยาบาลหรือภารกิจที่ได้รับมอบหมายเท่านั้น

ข้อ ๑๗ ข้อมูลส่วนบุคคลของบุคคลที่สาม ในกรณีที่ราชวิทยาลัยเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นจากผู้ปฏิบัติงานหรือผู้รับบริการ เช่น ข้อมูลของบุคคลในครอบครัวเพื่อการใช้สิทธิและสวัสดิการ ข้อมูลผู้ติดต่อในกรณีฉุกเฉิน หรือข้อมูลผู้รับรองการทำงาน ให้ส่วนงานตรวจสอบฐานทางกฎหมายและจัดให้มีการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลนั้นตามสมควรแก่กรณี และให้ผู้ที่ให้ข้อมูลรับรองว่าได้แจ้งหรือได้รับความยินยอมจากบุคคลดังกล่าวแล้ว

ข้อ ๑๘ การวิจัย การประมวลผลข้อมูลส่วนบุคคลเพื่อการศึกษาวิจัยต้องผ่านการพิจารณาของคณะกรรมการจริยธรรมการวิจัยในคน และต้องใช้ข้อมูลที่ผ่านการทำให้ไม่สามารถระบุตัวบุคคลได้เท่าที่จะกระทำได้ การส่งหรือแบ่งปันข้อมูลเพื่อการวิจัยกับหน่วยงานภายนอกต้องจัดทำข้อตกลงเป็นหนังสือ

ข้อ ๑๙ คำประกาศเกี่ยวกับความเป็นส่วนตัว ทุกส่วนงานต้องจัดให้มีคำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) สำหรับกิจกรรมที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล และแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมตามมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยอย่างน้อยต้องระบุประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม วัตถุประสงค์และฐานทางกฎหมาย ระยะเวลาเก็บรักษา ประเภทของบุคคลหรือหน่วยงานที่อาจได้รับการเปิดเผย สิทธิของเจ้าของข้อมูลส่วนบุคคล และช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ให้เผยแพร่ผ่านเว็บไซต์ของราชวิทยาลัยหรือช่องทางอื่นที่เข้าถึงได้โดยสะดวก และให้ทบทวนให้เป็นปัจจุบัน

ข้อ ๒๐ บันทึกรายการกิจกรรมการประมวลผล ทุกส่วนงานต้องจัดทำและปรับปรุงบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้เป็นปัจจุบันอย่างน้อยปีละหนึ่งครั้ง และส่งสำเนาให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ข้อ ๒๑ การเปิดเผยและการส่งต่อข้อมูลส่วนบุคคล การเปิดเผยหรือส่งข้อมูลส่วนบุคคลให้บุคคลหรือหน่วยงานภายนอก รวมถึงกรณีที่หน่วยงานของรัฐร้องขอ ต้องผ่านการพิจารณาฐานทางกฎหมายโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกับหน่วยงานที่รับผิดชอบด้านกฎหมายก่อนทุกครั้ง หนังสือขอความร่วมมือเพียงอย่างเดียวไม่ถือเป็นฐานทางกฎหมายที่ให้เปิดเผยข้อมูลได้ และให้เปิดเผยเพียงเท่าที่จำเป็นแก่วัตถุประสงค์ของการร้องขอ

ข้อ ๒๒ ผู้ประมวลผลข้อมูลส่วนบุคคลและคู่สัญญา การมอบหมายให้บุคคลภายนอกประมวลผลข้อมูลส่วนบุคคลแทนราชวิทยาลัย ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลเป็นหนังสือตามมาตรา ๔๐ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยอย่างน้อยต้องกำหนดขอบเขตการประมวลผล มาตรการรักษาความมั่นคงปลอดภัย การควบคุมผู้รับช่วงงาน หน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อราชวิทยาลัยภายในกำหนดเวลาที่เพียงพอต่อการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ข้อห้ามมิให้นำข้อมูลไปใช้เพื่อการอื่นรวมถึงการพัฒนาระบบปัญญาประดิษฐ์ และการคืนหรือทำลายข้อมูลเมื่อสิ้นสุดสัญญา

ข้อ ๒๓ การส่งหรือโอนข้อมูลไปยังต่างประเทศ การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องเป็นไปตามมาตรา ๒๘ และมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยต้องตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง และจัดให้มีมาตรการคุ้มครองที่เหมาะสมเป็นหนังสือก่อนการส่งหรือโอน

ข้อ ๒๔ ระยะเวลาเก็บรักษาและการทำลาย ให้ทุกส่วนงานกำหนดระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามความจำเป็นแก่วัตถุประสงค์หรือตามที่กฎหมายกำหนด และเมื่อพ้นกำหนดให้ลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ พร้อมจัดทำหลักฐานการดำเนินการ

หมวด ๔
มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

.....

ข้อ ๒๖ ราชวิทยาลัยต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ครอบคลุมมาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการทางกายภาพ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๒๗ การควบคุมการเข้าถึงและการกำหนดสิทธิผู้ใช้งาน ให้จัดให้มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์จัดเก็บข้อมูล การกำหนดสิทธิผู้ใช้งานตามหน้าที่ความรับผิดชอบโดยใช้หลักการให้สิทธิเท่าที่จำเป็น การบริหารจัดการการเข้าถึงของผู้ใช้งาน และการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานไว้เป็นลายลักษณ์อักษร

ข้อ ๒๘ การตรวจสอบย้อนหลังและการสอบทาน ให้จัดให้มีการบันทึกการเข้าถึง การแก้ไข และการเปิดเผยข้อมูลส่วนบุคคลในระบบสารสนเทศที่จัดเก็บข้อมูลอ่อนไหว และให้มีการสอบทานบันทึกดังกล่าวตามรอบระยะเวลาที่กำหนด โดยรายงานผลต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ข้อ ๒๙ การใช้อุปกรณ์และช่องทางสื่อสาร การประมวลผลข้อมูลส่วนบุคคลต้องกระทำผ่านระบบอุปกรณ์ และช่องทางสื่อสารที่ราชวิทยาลัยรับรองเท่านั้น การใช้อุปกรณ์ส่วนตัวหรือบริการภายนอกในการจัดเก็บหรือส่งข้อมูลส่วนบุคคลต้องได้รับอนุมัติและอยู่ภายใต้มาตรการที่กำหนด

ข้อ ๓๐ การทบทวนมาตรการ ให้ทบทวนมาตรการรักษาความมั่นคงปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานในลักษณะเดียวกัน ลักษณะและวัตถุประสงค์ของการประมวลผล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

หมวด ๕
สิทธิของเจ้าของข้อมูลส่วนบุคคล

.....

ข้อ ๓๑ สิทธิของเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล สิทธิขอให้โอนย้ายข้อมูล สิทธิคัดค้านการประมวลผล สิทธิขอให้ลบหรือทำลายข้อมูล สิทธิขอให้ระงับการใช้ข้อมูล สิทธิขอให้แก้ไขข้อมูลให้ถูกต้องเป็นปัจจุบัน สิทธิถอนความยินยอม และสิทธิร้องเรียน ทั้งนี้ ตามหลักเกณฑ์ที่กฎหมายกำหนด

ข้อ ๓๒ ช่องทางและระยะเวลาดำเนินการ เจ้าของข้อมูลส่วนบุคคลอาจใช้สิทธิผ่านช่องทางที่ราชวิทยาลัยกำหนด โดยให้ส่วนงานที่เกี่ยวข้องและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพิจารณาและแจ้งผลภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ในกรณีที่ปฏิเสธคำขอ ต้องบันทึกเหตุผลของการปฏิเสธและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

หมวด ๖
การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

.....

ข้อ ๓๓ การรายงานภายในองค์กร เมื่อผู้ใช้ข้อมูลส่วนบุคคลทราบหรือสงสัยว่ามีเหตุการละเมิดข้อมูลส่วนบุคคล ให้รายงานต่อหัวหน้าส่วนงานและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยทันทีผ่านช่องทางที่ราชวิทยาลัยกำหนด โดยไม่ต้องรอผลการตรวจสอบข้อเท็จจริงให้เสร็จสิ้นก่อน และห้ามมิให้ปกปิดหรือชะลอหรือประวิงเวลาการรายงาน

ข้อ ๓๔ การประเมินและการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประเมินความน่าเชื่อถือของข้อมูล ตรวจสอบข้อเท็จจริง ดำเนินการระงับหรือแก้ไขเหตุโดยทันที และประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด หากมีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริงและมิใช่กรณีที่ไม่มีความเสี่ยง ให้แจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

ข้อ ๓๕ การแจ้งเจ้าของข้อมูลส่วนบุคคลและการเยียวยา ในกรณีที่เหตุการละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า และให้ดำเนินมาตรการป้องกันมิให้เกิดเหตุในลักษณะเดียวกันซ้ำอีก พร้อมบันทึกเหตุการณ์และผลการดำเนินการไว้เป็นหลักฐาน

ข้อ ๓๖ การคุ้มครองผู้แจ้งเหตุ ผู้ซึ่งแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลหรือรายงานการไม่ปฏิบัติตามประกาศนี้โดยสุจริต ย่อมได้รับความคุ้มครองมิให้ถูกกลั่นแกล้งหรือได้รับการปฏิบัติที่ไม่เป็นธรรมอันเนื่องมาจากการแจ้งหรือรายงานนั้น

หมวด ๗
การสร้างความตระหนัก และการกำกับติดตาม

.....

ข้อ ๓๗ การอบรมและการสร้างความตระหนัก ให้ราชวิทยาลัยจัดให้มีการอบรมความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ปฏิบัติงานในราชวิทยาลัยทุกคนอย่างน้อยปีละหนึ่งครั้ง และจัดอบรมเฉพาะทางแก่ผู้ที่เข้าถึงข้อมูลอ่อนไหวและผู้ดูแลระบบสารสนเทศ ทั้งนี้ ให้ถือเป็นการพัฒนาบุคลากรตามข้อ ๗๖ ของข้อบังคับราชวิทยาลัยจุฬาภรณ์ ว่าด้วยการบริหารงานบุคคลของผู้ปฏิบัติงานในราชวิทยาลัย

จุฬาภรณ์ พ.ศ. ๒๕๖๙ ซึ่งทุกส่วนงานต้องจัดส่งผู้ปฏิบัติงานเข้ารับการอบรมตามที่ราชวิทยาลัยกำหนด และให้ผู้ใช้ข้อมูลส่วนบุคคลลงนามรับทราบหน้าที่ตามข้อ ๑๒ ทุกคน

ข้อ ๓๘ การกำกับติดตามและการตรวจสอบ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลติดตามและตรวจสอบการปฏิบัติตามประกาศนี้เป็นประจำ และรายงานผลต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชวิทยาลัยและคณะกรรมการบริหารอย่างน้อยปีละหนึ่งครั้ง ทั้งนี้ ทุกส่วนงานต้องให้ความร่วมมือและจัดส่งเอกสารหลักฐานตามที่ร้องขอ

ข้อ ๓๙ ผู้ปฏิบัติงานในราชวิทยาลัยมีหน้าที่ต้องปฏิบัติหน้าที่ให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อบังคับ ระเบียบ และประกาศของราชวิทยาลัยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ตามข้อ ๕๓ (๓) ของข้อบังคับราชวิทยาลัยจุฬาภรณ์ ว่าด้วยการบริหารงานบุคคลของผู้ปฏิบัติงานในราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๖๙ การฝ่าฝืนหรือไม่ปฏิบัติตามประกาศนี้ หากการกระทำนั้นเข้าลักษณะเป็นความผิดทางวินัย ให้ดำเนินการทางวินัย ตามข้อ ๕๕ ของข้อบังคับดังกล่าว และหากเป็นเหตุให้เกิดความเสียหายแก่ราชวิทยาลัยอย่างร้ายแรง อาจเป็นความผิดวินัยอย่างร้ายแรงตามข้อ ๕๖ (๖) ของข้อบังคับดังกล่าว ทั้งนี้ ไม่เป็นการตัดความรับผิดตามกฎหมายอื่นที่เกี่ยวข้อง

กรณีที่ส่วนงานตรวจพบว่ามีผู้ปฏิบัติงานภายในส่วนงานทำการฝ่าฝืนหรือไม่ปฏิบัติตามประกาศนี้ ให้รายงานต่อเลขาธิการราชวิทยาลัยจุฬาภรณ์เพื่อดำเนินการทางวินัยตามขั้นตอนและวิธีการที่กำหนดไว้ในข้อบังคับ ระเบียบ และประกาศ ของราชวิทยาลัยจุฬาภรณ์

สำหรับบุคคลตามข้อ ๖ วรรคสอง (๒) และ (๓) หากมีการฝ่าฝืนหรือไม่ปฏิบัติตามประกาศนี้ ให้เป็นไปตามข้อบังคับ ระเบียบ หรือสัญญาที่เกี่ยวข้อง แล้วแต่กรณี

ข้อ ๔๐ ให้มีการทบทวนความเหมาะสมของนโยบายตามประกาศนี้อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย โครงสร้างองค์กร ระบบสารสนเทศ หรือระดับความเสี่ยงที่มีนัยสำคัญ

ประกาศ ณ วันที่ ๖ เดือน ตุลาคม พ.ศ. ๒๕๖๙

(ศาสตราจารย์เกียรติคุณ นายแพทย์รัชตะ รัชตะนาวิน)

รักษาการรองเลขาธิการราชวิทยาลัยจุฬาภรณ์

ปฏิบัติหน้าที่แทนเลขาธิการราชวิทยาลัยจุฬาภรณ์