ประกาศมหาวิทยาลัยสวนดุสิต
เรื่อง แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๖๖

เพื่อให้การบริหารจัดการด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเพื่อให้ส่วนงาน หน่วยงาน หน่วยงานอิสระ และหน่วยงานภายใต้การกำกับของมหาวิทยาลัยที่มีชื่อเรียกเป็นอย่างอื่น ซึ่งในประกาศฉบับนี้จะรวมเรียกว่า **หน่วยงาน** สามารถใช้เป็นแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ตามที่คณะกรรมการขับเคลื่อนนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต และคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิตกำหนด ซึ่งในประกาศฉบับนี้จะรวมเรียกว่า **คณะกรรมการ**

อาศัยอำนาจตามความในมาตรา ๓๒ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๕๘ จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยสวนดุสิต เรื่อง แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ คำนิยาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ซึ่งอาจรวมถึงข้อมูลและสารสนเทศอื่น ๆ เช่น วันเดือนปีเกิด สัญชาติ เพศ ที่อาจรวมกันแล้ว สามารถระบุถึงผู้สมัครงานได้ ข้อมูลและสารสนเทศนี้ อาจจัดเก็บได้ในหลายรูปแบบ เช่น ทางอิเล็กทรอนิกส์ หรือแบบฟอร์มกระดาษ เป็นต้น

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือละเอียดอ่อน” หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยสวนดุสิต

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง มหาวิทยาลัยสวนดุสิต หมายรวมถึงหน่วยงานภายใต้การกำกับของมหาวิทยาลัย ผู้ปฏิบัติงานภายใต้คำสั่งหรือในนามมหาวิทยาลัยสวนดุสิต

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายถึง บุคคลที่มหาวิทยาลัยแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่ดูแล ให้คำแนะนำ

รักษาความลับ หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลในมหาวิทยาลัย ประสานงานและให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายที่ได้กำหนดไว้

"หน่วยงาน" หมายถึง ส่วนงาน หน่วยงาน หน่วยงานอิสระ และหน่วยงานภายใต้การกำกับของมหาวิทยาลัยที่มีชื่อเรียกเป็นอย่างอื่น

"ผู้ประสานงาน" หมายถึง ผู้ปฏิบัติงานที่ได้รับการแต่งตั้งให้ทำหน้าที่ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งในรูปแบบเอกสารหรืออิเล็กทรอนิกส์ ลบหรือทำลายข้อมูลส่วนบุคคล รับเรื่องและนำส่งเรื่องร้องเรียนเกี่ยวกับการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลต่อคณะกรรมการ และตรวจสอบการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล ร่วมกับคณะกรรมการ รวมถึงปฏิบัติหน้าที่ตามคำสั่งมหาวิทยาลัยสวนดุสิต

ข้อ ๔ วิธีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

(๑) วิธีการเก็บรวบรวมข้อมูลส่วนบุคคล

หน่วยงาน สามารถดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคล โดยจะต้องดำเนินการโดยผู้ประสานงานที่ได้รับการแต่งตั้ง ผ่านการอนุมัติจากหัวหน้าหน่วยงาน รวมถึงเอกสารอ้างอิง เช่น บัตรประจำตัวประชาชน ของผู้รับบริการเท่าที่จำเป็นต่อการประมวลผลและการดำเนินงานด้านต่าง ๆ ตามภารกิจหลักและวัตถุประสงค์ในการให้บริการ ที่ระบุไว้ใน**ประกาศความเป็นส่วนตัวสำหรับข้อมูลส่วนบุคคลและเอกสารแสดงความยินยอม** (Consent Form) โดยใช้แบบฟอร์มที่มหาวิทยาลัยกำหนดและได้รับอนุมัติแล้วเท่านั้น เป็นต้น

หน่วยงานต้องเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง จะเก็บรวบรวมจากแหล่งอื่นไม่ได้ หากต้องการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นสามารถดำเนินการได้บางกรณี เช่น ประโยชน์ต่อชีวิตหรือสุขภาพ โดยหน่วยงานสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ปฏิบัติงานภายในมหาวิทยาลัยหรือผู้รับบริการจากแหล่งอื่น เช่น ที่อยู่ปัจจุบัน จากกรมการปกครอง กระทรวงมหาดไทย เป็นต้น รวมเข้ากับข้อมูลส่วนบุคคลที่เจ้าของข้อมูลได้ให้ไว้ด้วยตนเอง เพื่อทำให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลมีความครบถ้วน ถูกต้อง และเป็นปัจจุบัน และช่วยให้หน่วยงานสามารถให้บริการตามภารกิจหลัก หรือเพื่อประโยชน์ต่อชีวิต หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล และเพื่อประโยชน์สาธารณะได้ดียิ่งขึ้น รวมถึงข้อมูลส่วนบุคคลจากสื่อสังคมออนไลน์ หรือที่ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๖๕

กรณีที่หน่วยงาน มีความจำเป็นต้องเก็บรวบรวม **ข้อมูลอ่อนไหว** เช่น ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด หน่วยงานจะต้องขอเอกสารแสดงความยินยอมจากเจ้าของข้อมูล เว้นแต่ได้รับการยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เช่น เพื่อป้องกันหรือระงับอันตรายต่อชีวิต รางกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ หรือเป็นการจำเป็นในการปฏิบัติตามกฎหมาย เป็นต้น และอื่น ๆ ที่ได้รับคำวินิจฉัยจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีที่หน่วยงาน ต้องการออกแบบฟอร์มหรือเอกสารแบบใหม่ที่ไม่ได้เป็นไปตามเอกสารที่ระบุไว้ในประกาศมหาวิทยาลัยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล แบบฟอร์มหรือเอกสารนั้นจะต้องได้รับการพิจารณาและทบทวนโดยคณะกรรมการก่อนนำไปใช้

(๒) การใช้และเปิดเผยข้อมูลส่วนบุคคล

การใช้และเปิดเผยข้อมูลส่วนบุคคล ภายในมหาวิทยาลัย จะต้องดำเนินการโดยผู้ประสานงานที่ได้รับการแต่งตั้ง ผ่านการอนุมัติจากหัวหน้าหน่วยงาน และเป็นการใช้ตามวัตถุประสงค์ที่ได้แจ้งไว้ในประกาศความเป็นส่วนตัวสำหรับข้อมูลส่วนบุคคลและเอกสารแสดงความยินยอมเท่านั้น ทั้งนี้ หัวหน้าหน่วยงานต้องกำกับดูแลผู้ประสานงานและผู้ปฏิบัติงานในหน่วยงานให้ปฏิบัติตามอย่างเคร่งครัด ในกรณีที่หน่วยงานใช้ข้อมูลส่วนบุคคลเพื่อทำธุรกรรมนอกเหนือจากที่ระบุไว้ในประกาศความเป็นส่วนตัวสำหรับข้อมูลส่วนบุคคลและเอกสารแสดงความยินยอม หน่วยงานจะต้องร่างธุรกรรมที่จะมีเพิ่มเติม ลงในแบบฟอร์มเอกสารแสดงความยินยอมที่มหาวิทยาลัยกำหนด เสนอต่อคณะกรรมการก่อนนำไปใช้ และจะต้องให้เจ้าของข้อมูลส่วนบุคคลพิจารณาและลงลายมือชื่อใน**เอกสารแสดงความยินยอม** ที่ได้รับการพิจารณาและทบทวนโดยคณะกรรมการแล้วไปเก็บรักษาไว้ในฐานข้อมูลหรือตามรูปแบบที่มหาวิทยาลัยกำหนด

การใช้และเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลหรือหน่วยงานภายนอก จะต้องดำเนินการ**ประเมิน**ก่อนส่งมอบข้อมูล **จัดเตรียม**ข้อมูลสำหรับส่งมอบข้อมูล ตามประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยผู้ประสานงานที่ได้รับการแต่งตั้ง ผ่านการอนุมัติจากหัวหน้าหน่วยงาน และต้องได้รับอนุมัติจากมหาวิทยาลัยตามลำดับ ก่อนการส่ง โอน ใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลหรือหน่วยงานภายนอก

(๓) การปฏิบัติต่อข้อมูลที่มีอยู่ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

หน่วยงานสามารถดำเนินการกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไว้ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบังคับใช้นั้นต่อไปได้ตามปกติโดยไม่ต้องส่งหนังสือขอความยินยอมให้เจ้าของข้อมูลพิจารณาให้ความยินยอมใหม่ โดย**ต้องเป็นไปตามวัตถุประสงค์เดิมเท่านั้น** แต่ต้องแจ้งวิธีการยกเลิกความยินยอมตามที่มหาวิทยาลัยกำหนด และประชาสัมพันธ์แจ้งให้เจ้าของข้อมูลทราบ เพื่อให้เจ้าของข้อมูลที่ไม่ต้องการให้เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย ทั้งนี้ หน่วยงานต้องแจ้งเตือนสิทธิและผลกระทบจากการยกเลิกความยินยอมให้แก่เจ้าของข้อมูลทราบก่อนยกเลิกความยินยอมนั้น

ข้อ ๕ ระยะเวลาการเก็บรักษา และการลบหรือทำลายข้อมูลส่วนบุคคล

(๑) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

หน่วยงานต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลที่ชัดเจนและสอดคล้องกับวัตถุประสงค์ของการใช้ข้อมูล โดยในกรณีทั่วไป ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลสูงสุดคือ ๑๐ ปี เว้นแต่จะมีระเบียบหรือกฎหมายกำหนดไว้เป็นอย่างอื่น เช่น เก็บรักษาไว้จนกว่าคดีความสิ้นสุด เป็นต้น

(๒) การลบหรือทำลายข้อมูลส่วนบุคคล

หน่วยงานต้องดำเนินการตามวิธีการและขั้นตอนการลบหรือทำลายข้อมูลส่วนบุคคลตามที่มหาวิทยาลัยกำหนด และบันทึกรายงานการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาจัดเก็บข้อมูลส่วนบุคคลตามแบบฟอร์มที่มหาวิทยาลัยกำหนด หรือปฏิบัติตามระเบียบและวิธีปฏิบัติที่มีการประกาศใช้ในมหาวิทยาลัย

การลบหรือทำลายข้อมูลส่วนบุคคลตามระยะเวลาที่กำหนด หัวหน้าหน่วยงานต้องทำหน้าที่ตรวจสอบรายการข้อมูลส่วนบุคคลที่ต้องดำเนินการลบหรือทำลายเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์ โดยกำหนดให้ผู้ประสานงานที่ได้รับการแต่งตั้งจัดทำรายการข้อมูลที่ต้องดำเนินการ

ลบหรือทำลาย เสนอต่อหัวหน้าหน่วยงาน และขออนุมัติดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลจากมหาวิทยาลัย

กรณีข้อมูลส่วนบุคคลที่มีการใช้เพื่อดำเนินคดีตามกฎหมาย และหรือมีการบังคับคดี หน่วยงานต้องเก็บรักษาข้อมูลส่วนบุคคลและฐานข้อมูลดังกล่าวไว้ต่อไปเพื่อใช้ในการดำเนินคดีจนกว่าคดีจะถึงที่สุด จึงจะสามารถลบหรือทำลายข้อมูลส่วนบุคคลนั้นได้

ข้อ ๖ การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

หน่วยงานต้องดำเนินการด้านการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ตามประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต อย่างเคร่งครัด

ข้อ ๗ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และการดำเนินการของหน่วยงานตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(๑) การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถยื่นขอใช้สิทธิในการได้รับแจ้ง เข้าถึง แก้ไข โอน ขอให้ลบหรือทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล ระงับการประมวลผล คัดค้าน และเพิกถอนความยินยอมได้ตามช่องทางและวิธีการที่มหาวิทยาลัยกำหนด

(๒) การดำเนินการของหน่วยงานตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลที่มีความประสงค์ขอใช้สิทธิ์ตามข้อ ๗(๑) สามารถยื่นขอใช้สิทธิด้วยตนเอง หรือมอบอำนาจให้ตัวแทนมาดำเนินการแทนได้ โดยให้ใช้**แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูล** พร้อมเอกสารประกอบคำร้องเพื่อยืนยันตัวตน ตามรูปแบบและวิธีการ ผ่านช่องทางที่มหาวิทยาลัยกำหนด โดยขั้นตอนการปฏิบัติดังนี้

ขั้นตอน	คำอธิบาย	ระยะเวลา
๑. การรับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล	เจ้าของข้อมูลส่วนบุคคลยื่นแบบคำขอใช้สิทธิตามรูปแบบและช่องทางที่มหาวิทยาลัยกำหนด	ไม่กำหนด
๒. การตรวจสอบตัวตนของผู้ยื่นคำขอใช้สิทธิ	หน่วยงานตรวจสอบตัวตนของผู้ยื่นคำขอ โดยพิจารณาจากเอกสารที่เกี่ยวข้องตามที่มหาวิทยาลัยกำหนด	ทันทีที่ได้รับแบบคำขอใช้สิทธิ
๓. การพิจารณาความถูกต้องของแบบขอใช้สิทธิ	หน่วยงานพิจารณาความถูกต้อง สมบูรณ์ของแบบคำขอใช้สิทธิ และเอกสารประกอบเป็นไปตามที่มหาวิทยาลัยกำหนด	ทันทีที่ได้รับแบบคำขอใช้สิทธิ
๔. การรวบรวมข้อมูลคำขอใช้สิทธิ	หน่วยงานต้องรวบรวมแบบคำขอพร้อมเอกสารประกอบ และนำส่งมายังคณะกรรมการเพื่อดำเนินการพิจารณาแบบคำขอ	โดยไม่ชักช้า แต่ไม่เกิน ๑ เดือนนับตั้งแต่วันที่ได้รับแบบคำขอใช้สิทธิ
๕. ดำเนินการตามสิทธิที่ยื่นคำขอ	คณะกรรมการพิจารณา และดำเนินการตามสิทธิที่ยื่นคำขอ และอาจต้องขยายระยะเวลาเนื่องจากมีความซับซ้อน หรือมีปริมาณแบบคำขอจำนวนมาก	โดยไม่ชักช้า แต่ไม่เกิน ๑ เดือน หรือ ๒ เดือน กรณีขยายระยะเวลา ทั้งนี้นับตั้งแต่วันที่ได้รับแบบคำขอใช้สิทธิ

ข้อ ๘ กรณีหน่วยงานตรวจพบความไม่ถูกต้องหรือความไม่สมบูรณ์ของข้อมูลส่วนบุคคล

หน่วยงานจะต้องแจ้งเจ้าของข้อมูลทราบ ในกรณีตรวจพบความไม่ถูกต้องหรือความไม่สมบูรณ์ของข้อมูลส่วนบุคคล จำเป็นต้องปรับปรุงหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลเพื่อประโยชน์ของเจ้าของข้อมูล และแจ้งให้เจ้าของข้อมูลดำเนินการยื่น**แบบคำขอใช้สิทธิ**ผ่านช่องทางที่มหาวิทยาลัยกำหนด ทั้งนี้ การแก้ไข ปรับปรุง เปลี่ยนแปลงข้อมูลส่วนบุคคล จะต้องได้รับการอนุมัติจากมหาวิทยาลัยก่อนการดำเนินการ

ข้อ ๙ การดำเนินการกรณีพบเหตุละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล

เมื่อเกิดเหตุละเมิดหรือมีการรั่วไหลของข้อมูลส่วนบุคคล ให้หน่วยงานดำเนินการ ดังนี้

(๑) ให้ผู้พบเหตุใช้แบบฟอร์มรายงานอุบัติการณ์ แจ้งเหตุการณ์ละเมิดหรือการรั่วไหลข้อมูลส่วนบุคคลแก่หัวหน้าหน่วยงานรับทราบเหตุ**ทันที**ที่ประสบเหตุ

(๒) ผู้ประสานงานที่ได้รับการแต่งตั้ง ดำเนินการรวบรวมรายละเอียด หลักฐาน และสาเหตุของการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล

(๓) ผู้ประสานงานที่ได้รับการแต่งตั้ง ทำการประเมินความเสี่ยงและวิเคราะห์ผลกระทบเบื้องต้นว่า มีความเสี่ยงต่อเจ้าของข้อมูลมากน้อยเพียงใด รวมทั้งเสนอแนะการแก้ไขเยียวยา

(๔) ผู้ประสานงานที่ได้รับการแต่งตั้ง ส่งเรื่องให้คณะกรรมการ

(๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต (DPO) ร่วมกับคณะกรรมการดำเนินการสอบทานการวิเคราะห์ความเสี่ยงของผลกระทบและมาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลของรายงานที่ได้รับ และให้ความเห็นชอบ อนุมัติผลการประเมินและมาตรการตอบสนอง

(๖) กรณีการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลมี**ความเสี่ยง และความเสี่ยงสูง** ที่จะกระทบต่อสิทธิของเจ้าของข้อมูล หรือก่อให้เกิดความเสี่ยงหายแก่เจ้าของข้อมูลส่วนบุคคล ให้คณะกรรมการจัดทำบันทึกรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต (DPO) เพื่อแจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลทราบ พร้อมแนวทางบรรเทาผลกระทบและแนวทางตอบสนองเพื่อหยุดยั้งการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล **ภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ**

กรณีที่หน่วยงานไม่ได้จัดทำรายงานภายในระยะเวลาที่กำหนด จะมีบทลงโทษจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลดังกล่าว**ไม่มีความเสี่ยง หรือมีความเสี่ยงต่ำ** ที่จะประทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกรายละเอียดของเหตุการณ์เพื่อเก็บไว้เป็นข้อมูลตรวจสอบย้อนหลังก็เพียงพอ **ไม่จำเป็นต้องแจ้ง**สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลทราบ

ข้อ ๑๐ การควบคุม กรณีมีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

กรณีที่หน่วยงานมีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคลภายนอก หน่วยงานจะต้องมีการทำ**เอกสารสัญญาและหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคล** ว่าต้องปฏิบัติตามข้อตกลงหรือตามคำสั่งของหน่วยงานในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น รวมทั้งหน้าที่ในการแจ้งเหตุแก่หน่วยงานในกรณีมีการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล โดยเอกสารสัญญาหรือข้อตกลงนั้นจะต้องได้รับการทบทวนและพิจารณาโดยคณะกรรมการที่เกี่ยวข้องก่อนนำไปใช้

ข้อ ๑๑ การบันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing หรือ RoP)

หน่วยงานจะต้องจัดทำบันทึกรายงานการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) ตามแบบฟอร์มและช่องทางที่มหาวิทยาลัยกำหนด ทั้งนี้ รายการประมวลผลข้อมูลส่วนบุคคล ประกอบด้วยหัวข้อต่าง ๆ ได้แก่

(๑) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล เช่น ชื่อและที่อยู่หน่วยงาน ข้อมูลการติดต่อ (ชื่อผู้ประสานงาน) เป็นต้น

(๒) ข้อมูลรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) เช่น ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม วัตถุประสงค์ของการเก็บรวบรวม ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล การใช้หรือเปิดเผยข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เป็นต้น

ข้อ ๑๒ ขั้นตอนการขออนุมัติเอกสาร แบบฟอร์ม และการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

สำหรับหน่วยงาน ที่มีความประสงค์ขออนุมัติเอกสาร แบบฟอร์ม และการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล รวมไปถึงการขออนุมัติเนื้อหาที่ต้องการระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด ต้องจัดทำบันทึกข้อความมายังคณะกรรมการที่เกี่ยวข้องก่อนนำไปใช้งานหรือก่อนนำไปดำเนินการต่อไป โดยมีขั้นตอนดังนี้

(๑) หน่วยงาน (ลงนามในบันทึกข้อความโดยหัวหน้าหน่วยงาน) เสนอร่างเอกสาร แบบฟอร์มหรือเนื้อหาที่ต้องการระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด หรือการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยระบุรายละเอียด เหตุผลประกอบการเสนอพิจารณา พร้อมแนบเอกสาร แบบฟอร์ม หรือรายละเอียดการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มายังเลขานุการคณะกรรมการขับเคลื่อนนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต ล่วงหน้าอย่างน้อย ๓๐ วันทำการ นับตั้งแต่วันที่หัวหน้าหน่วยงานลงนามในบันทึกข้อความ

(๒) เลขานุการคณะกรรมการขับเคลื่อนนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต รวบรวมเสนอต่อคณะกรรมการที่เกี่ยวข้องพิจารณา โดยใช้ระยะเวลารวมโดยประมาณ ๒๐ วันทำการ นับตั้งแต่วันที่เอกสารถึงเลขานุการคณะกรรมการขับเคลื่อนนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

(๓) เลขานุการคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เสนอมหาวิทยาลัยลงนามในเอกสาร แบบฟอร์มหรือเนื้อหาที่ต้องการระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด หรือการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และนำไปใช้หรือดำเนินการต่อไป (เอกสาร แบบฟอร์มหรือเนื้อหาที่ระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด หรือการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลบางประเภท มหาวิทยาลัยไม่ต้องลงนาม สามารถใช้งานหรือดำเนินการต่อไปได้ทันทีหลังจากได้รับการแจ้งผลการพิจารณานี้) ภายใน ๑๐ วันทำการ นับตั้งแต่วันที่กำหนดให้คณะกรรมการพิจารณาให้แล้วเสร็จ และแจ้งผลการพิจารณา พร้อมเอกสาร แบบฟอร์ม และการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลกลับไปยังหน่วยงานเพื่อนำไปใช้งานต่อไป

ทั้งนี้ เอกสาร แบบฟอร์มหรือเนื้อหาที่ระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด หรือการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ได้รับการอนุมัติจากคณะกรรมการแล้ว ต้องระบุวันที่ที่ได้รับ

การอนุมัติจากคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต ลงในส่วนหัวเอกสารหรือแบบฟอร์มทุกหน้า ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์ ตามรูปแบบข้อความ ดังนี้

เอกสารนี้ได้รับการอนุมัติ จากคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เมื่อวันที่.....

ตัวอย่าง
เอกสารนี้ได้รับการอนุมัติ จากคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เมื่อวันที่ ๒๕ มกราคม ๒๕๖๖

การใช้เอกสาร แบบฟอร์มหรือเนื้อหาที่ระบุลงในแบบฟอร์มมาตรฐานที่มหาวิทยาลัยกำหนด หรือการดำเนินการอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ยังไม่ได้รับการอนุมัติจากคณะกรรมการถือเป็นความผิด และหน่วยงานและหรือผู้ปฏิบัติงานนั้น จะได้รับโทษตามที่มหาวิทยาลัยกำหนด

ในกรณีที่หน่วยงานดำเนินการอื่นที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ในประกาศความเป็นส่วนตัวหรือเอกสารแสดงความยินยอม รวมไปถึงประกาศระเบียบ ข้อบังคับของมหาวิทยาลัย หรือกฎหมายอื่นที่กำหนด ต้องได้รับการอนุมัติจากคณะกรรมการ ตามขั้นตอนข้างต้นก่อนเท่านั้น

ข้อ ๑๔ การติดต่อสอบถาม

ในกรณีที่หน่วยงานมีข้อสงสัยหรือคำถามเกี่ยวกับแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต และในประกาศฉบับนี้ไม่ได้ระบุไว้ รวมถึงข้อเสนอแนะต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคล และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ของมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๖๕ รวมถึงประกาศอื่นที่เกี่ยวข้อง สามารถศึกษาเพิ่มเติมได้ที่เว็บไซต์ https://pdpa.dusit.ac.th/

ในกรณีที่ต้องการความช่วยเหลือเพิ่มเติม สามารถประสานงานผ่านเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย (Data Protection Officer: DPO) ได้ที่มหาวิทยาลัยสวนดุสิต เลขที่ ๒๙๕ ถนนนครราชสีมา แขวงดุสิต เขตดุสิต กรุงเทพมหานคร ๑๐๓๐๐ โทรศัพท์ ๐ ๒๒๔๔ ๕๕๕๕ อีเมล servicecenter@dusit.ac.th

ข้อ ๑๕ การทบทวนและปรับปรุงแนวปฏิบัติ

แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิตนี้ ครอบคลุมถึงแนวปฏิบัติต่อข้อมูลส่วนบุคคลของนักศึกษา ผู้เรียน นักเรียน ผู้ปฏิบัติงาน ผู้สมัครงาน ผู้สมัครเรียน และบุคคลหรือหน่วยงานภายนอกที่ติดต่อหรือรับบริการกับมหาวิทยาลัย รวมถึงผู้ใช้เว็บไซต์ แพลตฟอร์มออนไลน์ และช่องทางสื่อสังคมออนไลน์อื่น ๆ ของมหาวิทยาลัย

มหาวิทยาลัย ขอสงวนสิทธิ์ในการทบทวนและปรับปรุงแนวปฏิบัตินี้ตามที่เห็นสมควร ดังนั้น โปรดตรวจสอบแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิตอยู่เป็นประจำ

การเปลี่ยนแปลงใด ๆ จะมีผลทันทีเมื่อมหาวิทยาลัยเผยแพร่แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ที่แก้ไขดังกล่าวลงในเว็บไซต์ที่มหาวิทยาลัยกำหนด

ประกาศ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๖

(รองศาสตราจารย์ ดร.ศิโรจน์ ผลพันธิน)
อธิการบดีมหาวิทยาลัยสวนดุสิต