



ที่ พย ๐๐๒๓.๓/ว ๑๗๙๖

ศาลากลางจังหวัดพะเยา  
ถนนพหลโยธิน พย ๕๖๐๐๐

๒๕ มีนาคม ๒๕๖๙

เรื่อง แนวทางปฏิบัติในการขอรับข้อมูลที่ดินตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ใหม่อีกครั้ง

เรียน นายอำเภอ ทุกอำเภอ นายกเทศมนตรีเมืองพะเยา และนายกเทศมนตรีเมืองดอกคำใต้

อ้างถึง ๑. หนังสือจังหวัดพะเยา ด่วนที่สุด ที่ พย ๐๐๒๓.๓/ว ๓๔๕๑ ลงวันที่ ๔ เมษายน ๒๕๖๒

๒. หนังสือจังหวัดพะเยา ด่วนที่สุด ที่ พย ๐๐๒๓.๓/ว ๓๓ ลงวันที่ ๙ มกราคม ๒๕๖๓

สิ่งที่ส่งมาด้วย สำเนาหนังสือกรมส่งเสริมการปกครองท้องถิ่น ที่ มท ๐๘๐๘.๓/ว ๙๓๑  
ลงวันที่ ๒๕ กุมภาพันธ์ ๒๕๖๙

จำนวน ๑ ชุด

ตามที่ จังหวัดพะเยาได้แจ้งแนวทางปฏิบัติในการรับข้อมูลรูปแบบที่ดินและข้อมูลเอกสารสิทธิของที่ดินและสิ่งปลูกสร้างที่ตั้งอยู่ในเขตพื้นที่ขององค์กรปกครองส่วนท้องถิ่นจากกรมที่ดิน แก่เทศบาลและองค์การบริหารส่วนตำบล เพื่อเตรียมความพร้อมในการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง ตามพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ความละเอียดตามหนังสือที่อ้างถึง นั้น

จังหวัดพะเยาได้รับแจ้งจากกรมส่งเสริมการปกครองท้องถิ่นว่า กรมที่ดินได้ขอความอนุเคราะห์แจ้งแนวทางปฏิบัติในการขอรับข้อมูลตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ กรณีข้อมูลท้องที่กรปกครองส่วนท้องถิ่นได้รับไปแล้วสูญหาย เนื่องจากเป็นกรณีที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ จึงขอความร่วมมืออำเภอแจ้งองค์กรปกครองส่วนท้องถิ่นทราบและถือปฏิบัติ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อพิจารณาดำเนินการ สำหรับเทศบาลเมืองพะเยาและเทศบาลเมืองดอกคำใต้ ขอแจ้งมาเพื่อทราบและถือปฏิบัติด้วย

ขอแสดงความนับถือ

(นายสมศักดิ์ แก้วเสนา)  
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน  
ผู้ว่าราชการจังหวัดพะเยา

สำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัด  
กลุ่มงานส่งเสริมและพัฒนาท้องถิ่น  
โทร./โทรสาร ๐ ๕๔๔๔ ๙๖๒๔ ต่อ ๑๔

๑๓-๑๖-๖๖



ที่ มท ๐๘๐๘.๓/ว ๙๓๑

กรมส่งเสริมการปกครองท้องถิ่น  
ถนนนครราชสีมา เขตดุสิต กทม. ๑๐๓๐๐

๒๕ กุมภาพันธ์ ๒๕๖๙

เรื่อง แนวทางปฏิบัติในการขอรับข้อมูลที่ดินตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ใหม่อีกครั้ง

เรียน ผู้ว่าราชการจังหวัด ทุกจังหวัด

อ้างถึง ๑. หนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนที่สุด ที่ มท ๐๘๐๘.๓/ว ๑๓๓๒ ลงวันที่ ๒๘ มีนาคม ๒๕๖๒  
๒. หนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนที่สุด ที่ มท ๐๘๐๘.๓/ว ๕๓๖๑ ลงวันที่ ๒๗ ธันวาคม ๒๕๖๒

สิ่งที่ส่งมาด้วย สำเนาหนังสือกรมที่ดิน ที่ มท ๐๕๒๕.๓/๑๓๑๘ ลงวันที่ ๒๒ มกราคม ๒๕๖๙ จำนวน ๑ ฉบับ

ตามที่ กรมส่งเสริมการปกครองท้องถิ่นได้แจ้งแนวทางปฏิบัติในการรับข้อมูลรูปแบบแปลงที่ดิน และข้อมูลเอกสารสิทธิของที่ดินและสิ่งปลูกสร้างที่ตั้งอยู่ในเขตพื้นที่ขององค์กรปกครองส่วนท้องถิ่นจากกรมที่ดิน แก่เทศบาล องค์การบริหารส่วนตำบล และเมืองพัทยา เพื่อเตรียมความพร้อมในการจัดเก็บภาษีที่ดิน และสิ่งปลูกสร้าง ตามพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ความละเอียดตามหนังสือที่อ้างถึง นั้น

กรมส่งเสริมการปกครองท้องถิ่นขอเรียนว่า กรมที่ดินได้ขอความอนุเคราะห์แจ้งแนวทางปฏิบัติในการขอรับข้อมูลตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ กรณีข้อมูลที่ต้องกรปกรองส่วนท้องถิ่นได้รับไปแล้วสูญหาย เนื่องจากเป็นกรณีที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ จึงขอความร่วมมือจังหวัดแจ้งองค์กรปกครองส่วนท้องถิ่นทราบและถือปฏิบัติ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายธนนท์ พรพืภาส)

รองอธิบดี ปฏิบัติราชการแทน

อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

สำนักบริหารการคลังท้องถิ่น

กลุ่มงานนโยบายการคลังและพัฒนารายได้

โทร. ๐-๒๒๔๑-๙๐๐๐ ต่อ ๑๔๓๓

ไปรษณีย์อิเล็กทรอนิกส์ saraban@dla.go.th



สิ่งที่ส่งมาด้วย



# บันทึกข้อความ

กรมส่งเสริมการปกครองท้องถิ่น  
 เลขรับ..... 3๗47  
 วันที่ 26 ม.ค. 2569  
 เวลา.....

ส่วนราชการ กรมที่ดิน ศูนย์ข้อมูลแผนที่รูปแปลงที่ดิน (ครท.) โทร. ๐ ๒๕๐๓ ๓๓๖๕

ที่ มท ๐๕๒๕.๓ / ๑๙๑๗ วันที่ ๒๗ มกราคม ๒๕๖๙

เรื่อง แนวทางปฏิบัติในการขอรับข้อมูลที่ดินตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง

พ.ศ. ๒๕๖๒ ใหม่อีกครั้ง

สำนักบริหารการคลังท้องถิ่น  
 เลขรับ..... 171  
 วันที่ ๒๕ ม.ค. ๒๕๖๙  
 เวลา.....

เรียน อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

ตามหนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนที่สุด ที่ มท ๐๘๐๘.๓/ว๑๓๓๒ ลงวันที่ ๒๘ มีนาคม ๒๕๖๒ และ ด่วนที่สุด ที่ มท ๐๘๐๘.๓/ว๕๓๖๑ ลงวันที่ ๒๗ ธันวาคม ๒๕๖๒ แจ้งจังหวัดเพื่อแจ้งเทศบาล เมืองพัทยา และองค์การบริหารส่วนตำบล กรณีการเตรียมความพร้อมและการรับข้อมูลที่ดินตามมาตรา ๙๒ และมาตรา ๑๐ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ความละเอียดแจ้งแล้ว นั้น

กรมที่ดินได้รับการประสานจากองค์กรปกครองส่วนท้องถิ่น (อปท.) หลายแห่ง แจ้งความประสงค์ขอข้อมูลเกี่ยวกับที่ดินซึ่งเป็นข้อมูลรูปแปลงที่ดินและข้อมูลเอกสารสิทธิของที่ดินและสิ่งปลูกสร้างที่ตั้งอยู่ในเขตพื้นที่ขององค์กรปกครองส่วนท้องถิ่นแต่ละแห่งเพื่อใช้ในการเตรียมการจัดเก็บภาษี ตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ โดยระบุเหตุผลความจำเป็น เช่น การทำรหัสผ่านสำหรับเปิดข้อมูลสูญหาย การลาออกของเจ้าหน้าที่ที่รับผิดชอบ เครื่องคอมพิวเตอร์ที่จัดเก็บข้อมูลชำรุดทำให้ข้อมูลสูญหาย หรือการเปลี่ยนแปลงอีเมลที่ใช้รับข้อมูล อันเป็นเหตุให้ อปท. ไม่สามารถนำข้อมูลที่ได้รับไปแล้วตามมาตรา ๙๒ มาใช้ดำเนินงานได้ ซึ่งตามพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ มาตรา ๙๒ กำหนดให้กรมที่ดินจัดส่งข้อมูลรูปแปลงที่ดินและข้อมูลเอกสารสิทธิของที่ดินและสิ่งปลูกสร้างให้ อปท. ในเขตพื้นที่การปกครองที่รับผิดชอบ โดยเป็นการจัดส่งให้เพียงครั้งเดียวภายใน ๖๐ วัน นับแต่วันที่พระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ ใช้บังคับ ซึ่งกรมที่ดินได้จัดส่งให้ อปท. ทุกแห่งไปครบถ้วนแล้ว ดังนั้น เพื่อให้การปฏิบัติงานเป็นไปด้วยความชัดเจน สอดคล้องกับระเบียบ และข้อกฎหมายที่เกี่ยวข้อง จึงขอความอนุเคราะห์จากกรมส่งเสริมการปกครองท้องถิ่นแจ้งแนวทางปฏิบัติเกี่ยวกับการขอรับข้อมูลตามมาตรา ๙๒ แห่งพระราชบัญญัติภาษีที่ดินและสิ่งปลูกสร้าง พ.ศ. ๒๕๖๒ กรณีข้อมูลที่ดินที่ได้รับไปแล้วสูญหาย เนื่องจากเป็นกรณีที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ให้แก่ อปท. ทุกแห่งทราบ ดังนี้

๑. กรณีมีการเปลี่ยนผู้ดูแลระบบ การเปลี่ยนแปลง E-mail หรือการทำรหัสสำหรับเปิดข้อมูลสูญหาย อปท. จะต้องลงทะเบียนผ่านแพลตฟอร์มกลาง (Platform) เพื่อการบูรณาการระบบทะเบียนทรัพย์สินโครงการบูรณาการระบบทะเบียนทรัพย์สิน (กรมที่ดิน) เพื่อขอรับรหัสผ่านในการเปิดข้อมูล โดยกรมที่ดินจะจัดส่งรหัสเดิมสำหรับเปิดข้อมูลให้แก่ อปท. อีกครั้งหนึ่ง

๒. กรณีการขอรับข้อมูลตามมาตรา ๙๒ ใหม่อีกครั้ง เนื่องจากข้อมูลสูญหายไม่ว่าจะสูญหายด้วยสาเหตุใดก็ตาม อปท. จะต้องดำเนินการตามมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดว่า “มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้ (๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น

/ หรือเมื่อ...

หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด” และประกาศคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ซึ่งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธ.) ได้มีการกำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติ ของผู้ควบคุมข้อมูลไว้แล้ว โดยกรมส่งเสริมการปกครองท้องถิ่นสามารถดาวน์โหลดเอกสารได้ที่ QR Code ท้ายหนังสือฉบับนี้

ทั้งนี้ เมื่อได้มีการแจ้งเวียนแนวทางปฏิบัติให้ อปท. ดำเนินการตามมาตรา ๓๗ (๑) แห่งพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการ รักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ แล้ว กรุณาแจ้งให้กรมที่ดินทราบเพื่อใช้ ในการพิจารณาจัดส่งข้อมูลให้ อปท. อีกครั้งหนึ่ง โดยเป็นการดำเนินการตามพระราชบัญญัติการบริหารงาน และการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ด้วย

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการ



(นายเจนกิจ เชษฐวานิชย์)  
รองอธิบดี ปฏิบัติราชการแทน  
อธิบดีกรมที่ดิน



ศูนย์ข้อมูลแผนที่รูปแปลงที่ดิน  
โทร./โทรสาร ๐ ๒๕๐๓ ๓๓๖๕

<https://portal.dol.go.th/zNkDic>  
เอกสารที่เกี่ยวข้อง

0143299216  
0645894770

กลุ่มสาระการเรียนรู้ภาษาไทย  
เลขที่ 70  
เลขที่ ๒๖ ม.ค. ๒๕๖๓  
16.10 พ.

เอกสารแนบ ๓

นาย ชรินทร์ สัจจามัน  
พราม

- หนังสือเรียน.....
- ผ.บท.....
- ผ.นโยบาย.....
- ผ.พัฒนารายได้ เงินค่าจ้าง/บอกรื้อ + ภาษี

*(Handwritten signature)*

(นายชรินทร์ สัจจามัน)  
ผอ.ก.ง.คร.

๒๖ ม.ค. ๒๕๖๓

## ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความมั่นคงปลอดภัย” หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ

(information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(๔) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการอ้างไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(๕) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตราการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

(๖) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยดำเนินการดังต่อไปนี้ อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need-to-know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning) การบริหารจัดการสิทธิการเข้าถึง

ตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นกรกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ ๔ เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็น ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๖ ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำตามข้อ ๔ โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ ๗ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคล จะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

ข้อ ๘ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕

เจียรชัย ณ นคร

ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล  
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

สพร. กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจาก  
มาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีทั้งหมด  
5 ข้อ ดังนี้

**มาตรา 37 (1)** จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้  
เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน  
มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษา  
ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

ให้อธิบายมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมอย่างน้อย 3 ประเด็นดังนี้

- 1) การธำรงไว้ซึ่งความลับ (confidentiality)
- 2) ความถูกต้องครบถ้วน (integrity) และ
- 3) สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

โดยอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

1. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

1.1 มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการ  
จัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น  
กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มี  
สิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง

ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่  
อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

1.2 มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของ  
ผู้ใช้งาน (user responsibilities) แบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข  
เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

2. มาตรการป้องกันด้านเทคนิค (technical safeguard)

- a. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
  - b. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย
  - c. จัดให้มีระบบสำรองและกักเก็บข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง
3. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)
- 3.1 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อกประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก  
ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมีขอบ
  - 3.2 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

---

**มาตรา 37 (2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ**

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วย การดำเนินการ ดังต่อไปนี้

1. การประเมินก่อนส่งมอบข้อมูล
  - a. ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล
  - b. ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลไว้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่

หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้เฉพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว 13 หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้เฉพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงพอการนำไปใช้ประโยชน์หรือไม่

## 2. เมื่อส่งมอบข้อมูล

- จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน
- ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน
- แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

## 3. หลังส่งมอบข้อมูล

- ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก 3 เดือน 6 เดือน หรือ 1 ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้น ลบทำลายข้อมูล
- กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากัน โดยอัตโนมัติตลอดเวลา

---

**มาตรา 37 (3)** จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

- ติดตามสม่ำเสมอ (เช่น ทุกสัปดาห์ หรือ ทุกเดือน) ว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy

Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

2. กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอลอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี
3. การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

---

**มาตรา 37 (4)** แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและช้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

สิ่งที่ดำเนินการอย่างน้อยควรประกอบด้วย การดำเนินการ ดังต่อไปนี้

1. กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของสำนักงานให้ชัดเจน เช่น การส่งอีเมลล์ และ แจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน
2. กำหนดวิธีปฏิบัติให้ตัวแทนสำนักงานต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง (นับแต่ทราบเหตุ)
3. การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น
  - a. ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพื่งบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ
  - b. ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ 1 เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน 72 ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย
  - c. ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลล์ไปยังผู้รับผิดชอบลาต ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง 2 คน ใน 15 คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตาม แม้ข้อมูลสุขภาพ จะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพื่งบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

หมายเหตุ กรณีตัวอย่างและวิธีปฏิบัติข้างต้นอ้างอิงจาก Guidelines 01/2021 on Examples regarding Data Breach Notification สามารถศึกษาวิธีการปฏิบัติเพิ่มเติมได้จาก [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en)

---

**มาตรา 37 (5)** ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในข้อนี้ ยังไม่มีความจำเป็นที่ สพร. ต้องดำเนินการใด ๆ