

มาตรการแจ้งการละเมิดข้อมูลส่วนบุคคลภายใต้
กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ว่าที่ร้อยตรีสุทธิพงษ์ โพธิ์ถาวร

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์
สถาบันบัณฑิตพัฒนบริหารศาสตร์

2566

บทคัดย่อ

ชื่อการค้นคว้าอิสระ	มาตรการแจ้งการละเมิดข้อมูลส่วนบุคคลภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล
ชื่อผู้เขียน	ว่าที่ร้อยตรีสุทธิพงษ์ โพธิ์ถาวร
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
ปีการศึกษา	2566

การแจ้งการละเมิดข้อมูลส่วนบุคคลเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องดำเนินการ มาตรการและแจ้งการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด (โดยไม่ชักช้า ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้) สิทธิในการได้รับการแจ้งการละเมิดข้อมูลส่วนบุคคลจึงเป็นสิทธิอย่างหนึ่งของเจ้าของข้อมูลส่วนบุคคลควรได้รับ อย่างไรก็ตาม กฎหมาย ลำดับรองและแนวปฏิบัติที่เกี่ยวข้องกับการแจ้งการละเมิดข้อมูลส่วนบุคคลไม่ได้อธิบายหรือ ยกตัวอย่างให้ทราบว่าเมื่อใดที่จะถือว่าผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคล

ดังนั้น การที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ไม่มีแนวปฏิบัติที่ชัดเจน ย่อมทำให้เกิดความไม่ชัดเจนในทางปฏิบัติเกี่ยวกับระยะเวลาในการแจ้งการละเมิดข้อมูลส่วนบุคคลว่า “ระยะเวลาใดที่จะถือว่าผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคล” อาจทำให้ผู้ควบคุมข้อมูลส่วนบุคคลถูกลงโทษปรับทางปกครองเนื่องจากไม่แจ้งการละเมิดข้อมูลส่วนบุคคล ภายในระยะเวลาที่กฎหมายกำหนด ในทางตรงกันข้ามอาจทำให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ ประโยชน์จากความไม่ชัดเจนในทางปฏิบัติดังกล่าวแจ้งการละเมิดข้อมูลส่วนบุคคลโดยไม่ชอบด้วย กฎหมายหรือแจ้งการละเมิดข้อมูลส่วนบุคคลล่าช้าทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย

การค้นคว้าอิสระฉบับนี้ ผู้เขียนได้ทำการศึกษา รวบรวม วิเคราะห์และเปรียบเทียบ หลักเกณฑ์ทางกฎหมายและมาตรการเกี่ยวกับการแจ้งการละเมิดข้อมูลส่วนบุคคล และแนวทาง ปฏิบัติที่ชัดเจนในกรณีที่จะถือว่าผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคล ระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ สหภาพยุโรป (General Data Protection Regulation หรือ GDPR) รวมถึงแนวปฏิบัติการแจ้งการ ละเมิดข้อมูลส่วนบุคคลของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (European

(4)

Data Protection Board หรือ EDPB) เพื่อผลักดันให้เกิดแนวปฏิบัติที่ชัดเจนเกี่ยวกับระยะเวลาที่จะถือว่าผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคลและทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถแจ้งการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนดอย่างเหมาะสมและถูกต้องตามกฎหมาย

ABSTRACT

Title of Independent Study	Data Breach Notification Measures under the Personal Data Protection Laws
Author	Acting Sub Lt. Sutthiphong Phothaworn
Degree	Master of Laws
Year	2023

Notification of personal data breaches is the responsibility of the data controller, who must take measures and notify of the breach within the timeframe prescribed by law (without delay, within 72 hours from becoming aware of it). The right to be notified of personal data breaches is therefore one of the rights that the data subject should receive. However, subsidiary legislation and relevant practices regarding personal data breach notification do not explicitly explain or provide examples of when it is considered that the data controller has become aware of the personal data breach. As a result, the Personal Data Protection Commission (PDPC) lacks clear guidelines on the timeframe for notifying personal data breaches, specifically, “At what point is it considered that the data controller is aware of the personal data breach.” This ambiguity may lead to data controllers being fined by the regulatory authority for not notifying personal data breaches within the legally specified timeframe. Conversely, it may allow data controllers to exploit the lack of clarity in guidelines by notifying personal data breaches without legal approval or delaying notification, causing harm to the data subjects. This independent study aims to address this gap by examining, collecting, analyzing, and comparing legal criteria and measures for personal data breach notification, as well as clear guidelines in cases when it is considered that the data controller is aware of the personal data breach. It compares the Personal Data Protection Act of Thailand with the General Data Protection Regulation (GDPR) of

(6)

the European Union, including the notification guidelines provided by the European Data Protection Board (EDPB). The goal is to advocate for the establishment of clear guidelines regarding the timeframe for considering when the data controller is aware of a personal data breach and to enable data controllers to notify personal data breaches within the legally specified timeframe appropriately and accurately according to the law.