การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รุ่นที่ 1

นางสาวกานต์มณี จันทร์ขาว นักวิชาการเกษตรชำนาญการ กองเทคโนโลยีชีวภาพทางดิน
ที่มา: หลักสูตร “การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” รุ่นที่ 1 โดย วิทยากรจากบริษัท ไอทีคอมพาเนี่ยน จำกัด ณ ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และภูมิสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร วันที่ 31 มกราคม 2566

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว กระทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

1. การคุ้มครองข้อมูลส่วนบุคคล

บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียงและครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่งหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

2. วัตถุประสงค์การคุ้มครองข้อมูลส่วนบุคคลของไทย

2.1 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพโดยกำหนดหน้าที่และความรับผิดชอบที่เหมาะสม

2.2 เพื่อให้มีมาตรการเยียวยาจากการถูกละเมิดสิทธิให้ข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

2.3 เพื่อส่งเสริมการใช้ข้อมูลในการพัฒนานวัตกรรมอย่างมั่นคงปลอดภัย

2.4 เพื่อสร้างความโปร่งใสและความเป็นธรรมในการใช้ข้อมูลส่วนบุคคล

3. ข้อมูลส่วนบุคคล ได้แก่ บัตรประชาชน ภาพถ่าย เสียงพูด IP Address/ Cookies เอกสารข้อมูลส่วนบุคคล ไฟล์วิดีโอ ข้อมูลในอุปกรณ์ อิเล็คทรอนิกส์ ลายมือ

4. สาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.1 เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น

4.2 ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล

4.3 เจ้าของข้อมูลมีสิทธิ์ถอนความยินยอม ขอให้ลบหรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล

5. สิทธิของเจ้าของข้อมูลส่วนบุคคล

5.1 สิทธิได้รับการแจ้งให้ทราบ

5.2 สิทธิขอเข้าถึงข้อมูลส่วนบุคคล

5.3 สิทธิในการขอให้โอนข้อมูลส่วนบุคคล

5.4 สิทธิคัดค้านการเก็บรวบรวมให้ หรือเปิดเผยข้อมูลส่วนบุคคล

5.5 สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล

5.6 สิทธิขอให้ระงับการใช้ข้อมูล

5.7 สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล

6. ข้อควรรู้ พ.ร.บ.ข้อมูลส่วนบุคคลฯ

6.1 การเก็บข้อมูล การใช้ข้อมูล เปิดเผยข้อมูลควรได้รับความยินยอมเสมอ

การกระทำใดๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล มาตรา 83 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 3,000,000 บาท

6.2 การขอความยินยอม ต้องทำเป็นหนังสือหรือผ่านระบบออนไลน์ตามแบบที่กำหนดไว้

การกระทำใดๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้ผ่านการขอความยินยอมตามรูปแบบที่ถูกต้อง มาตรา 82 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

6.3 การเก็บข้อมูล ต้องแจ้งรายละเอียดและแจ้งสิทธิต่อเจ้าของข้อมูล

การกระทำใดๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้แจ้งวัตถุประสงค์ แจ้งรายละเอียด และแจ้งสิทธิของเจ้าของข้อมูล มาตรา 82 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

6.4 ต้องเก็บข้อมูลจากเจ้าของข้อมูลเท่านั้นห้ามเก็บจากแหล่งอื่น

เก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้จากเจ้าของข้อมูลโดยตรง โดยไม่มีข้อยกเว้นให้เก็บข้อมูลได้ มาตรา 83 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 3,000,000 บาท

6.5 ธุรกิจใหญ่ ต้องมี “เจ้าหน้าที่คุ้มครองข้อมูล” ของตัวเอง

ผู้ประกอบการที่ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา 85 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

6.6 การเก็บและใช้ข้อมูล ถูกตรวจสอบโดยคณะกรรมการผู้เชี่ยวชาญ

ผู้ประกอบกิจการได้รับคำสั่งจากคณะกรรมการผู้เชี่ยวชาญแล้วไม่ให้ความร่วมมือ ไม่มาชี้แจงข้อเท็จจริง มาตรา 89 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 500,000 บาท

6.7 ข้อมูลคนตาย กฎหมายไม่คุ้มครอง

6.8 บริษัทต่างชาติ คุ้มครองข้อมูลของคนในประเทศ ไม่ว่าบริษัทตั้งอยู่ที่ใด

6.9 ฝ่าฝืนกฎหมายนี้ อาจโดน “ค่าเสียหายเชิงลงโทษ” จ่ายสองเท่า

7. ประเภทภัยคุกคาม และความเสี่ยง

7.1 ภัยจากการบุกรุกจากภายนอก

7.1.1 ความเสี่ยงข้อมูลส่วนบุคคล

7.1.2 การรั่วไหลของข้อมูลบนคลาวด์

7.1.3 ภัยคุกคามจาก Call Center

7.1.4 การตกเป็นข่าว หรือเรื่องอื้อฉาวในสื่อสังคมออนไลน์

7.2 ภัยจากการใช้งานไม่เหมาะสม

7.2.1 ความไม่ปลอดภัยในอุปกรณ์

7.2.2 ภัยจากการนำปัญญาประดิษฐ์ไปใช้

7.2.3 การถูกฉ้อฉลผ่านการจ่ายเงินออนไลน์

7.2.4 ปัญหาการละเมิดต่อกฎหมาย กฎระเบียบความมั่นคงปลอดภัยทางไซเบอร์

7.2.5 การละเมิดข้อมูลส่วนบุคคล

7.3 ภัยจากการขาดความเข้าใจ และการดำเนินการไม่มีประสิทธิภาพ

7.3.1 สถานะของความปลอดภัยทางไซเบอร์ที่เหมาะสม

7.3.2 โลกการเงินคริปโต และบล็อกเชน (Blockchain)

7.3.3 การเปลี่ยนแปลงของโลกดิจิทัล และการเปลี่ยนแปลงของความมั่นคงปลอดภัย

ในปี 2554 ที่ผ่านมา สถิติภัยคุกคามในการค้นหาของไทยเซิร์ตมากที่สุด คือภัยคุกคามประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ ซึ่งเป็นเรื่องเกี่ยวกับ **Phishing** ดังนั้นควรรู้จักและระวังภัยชนิดนี้

Phishing หมายถึง เทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น

ข้อควรระหวังสำหรับ Phishing

1. อีเมลที่ขอข้อมูลส่วนบุคคล เปิดอ่าน แต่ห้ามคลิก
2. อีเมลที่ไม่น่าไว้ใจ
3. การปลอมอีเมล
4. ระมัดระวังสิ่งที่แนบมา
5. ระวังเรื่องข้อความ หรืออีเมลความเร่งด่วน
6. เว็บไซต์ปลอม
7. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย