# การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง: กรณีศึกษาสหภาพยุโรป

# Risk-Based Approach to Personal Data Security Measures: A Case Study of the European Union

ปกรณ์ วิญญูหัตถกิจ[1*]
Pakorn Winyuhuttakit[1*]

**บทคัดย่อ**

ปัจจุบันพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามระดับความเสี่ยง แต่ไม่ได้กำหนดแนวทางการจัดทำมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามระดับความเสี่ยงไว้ ทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยยังขาดความชัดเจนในเรื่องหลักการประเมินความเสี่ยงและกลไกการนำไปปฏิบัติที่เป็นรูปธรรม จากการศึกษากฎหมาย GDPR ของสหภาพยุโรป พบว่ามีการกำหนดให้จัดทำมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามระดับความเสี่ยงเช่นกัน โดยใช้เครื่องมือสำคัญ คือ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) พร้อมจัดทำแนวปฏิบัติเกี่ยวกับกระบวนการขั้นตอนการทำ DPIA ดังนั้นประเทศไทยจึงควรดำเนินการในแนวทางเดียวกับสหภาพยุโรป โดยจัดทำแนวปฏิบัติหรือคู่มือเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่กำหนดกระบวนการขั้นตอนการทำ DPIA อย่างเป็นระบบ เพื่อให้องค์กรต่าง ๆ มีแนวทางที่น่าเชื่อถือในการนำไปปฏิบัติได้อย่างเป็นรูปธรรม

**คำสำคัญ:** ข้อมูลส่วนบุคคล, มาตรการรักษาความมั่นคงปลอดภัย, ระดับความเสี่ยง, การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

**Abstract**

[1] ผู้ช่วยศาสตราจารย์ ดร., คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย
[1] Assistant Dr., School of Law, The University of the Thai Chamber of Commerce (UTCC)
* ผู้ประสานงานนิพนธ์ e-mail : pakorn_win@utcc.ac.th

Currently, the Personal Data Protection Act B.E. 2562 requires Data Controllers and Data Processors to implement appropriate security measures in accordance with risk levels. However, the Act does not prescribe specific guidelines for establishing such measures based on risk levels which results in a lack of clarity regarding risk assessment principles and concrete implementation mechanisms within Thailand's data protection framework. A comparative study of the EU General Data Protection Regulation (GDPR) reveals a similar requirement for implementing security measures based on risk levels. Crucially, the GDPR utilizes the Data Protection Impact Assessment (DPIA) as a primary tool, supported by comprehensive procedural guidelines. Therefore, Thailand should align its approach with the European Union by establishing comprehensive guidelines or a manual on personal data security measures. Such guidance should prescribe a systematic process for conducting DPIA as well as providing organizations with a reliable and practical framework for implementation.

**Keywords:** Personal Data, Security Measure, Risk Level, DPIA

**บทนำ**

ในยุคดิจิทัล ข้อมูลส่วนบุคคลของประชาชนมีความสำคัญอย่างมากต่อการดำเนินกิจกรรมของภาครัฐและภาคเอกชน และมีความเสี่ยงที่ข้อมูลดังกล่าวจะถูกละเมิดภายใต้กิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กรที่นำข้อมูลดังกล่าวไปใช้ประโยชน์ ไม่ว่าองค์กรนั้นจะมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล[2] หรือผู้ประมวลผลข้อมูลส่วนบุคคล[3] ประเทศต่าง ๆ ในโลกจึงพยายามพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองสิทธิของประชาชนซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล โดยในปี ค.ศ. 2016 สหภาพยุโรปได้จัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับสำคัญเพื่อเป็นต้นแบบให้ประเทศต่าง ๆ ในสหภาพยุโรป ได้แก่ Regulation (EU) 2016/679[4] หรือที่เรียกว่า GDPR (General Data Protection Regulation) ซึ่งกฎหมายดังกล่าวได้วางหลักการสำคัญให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง (Risk-based approach)[5] โดยเครื่องมือสำคัญที่ทำให้สามารถระบุความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคลและกำหนด

[2] หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

[3] หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

[4] Regulation (EU) 2016/679 (GDPR) ได้รับการลงมติรับรองเมื่อวันที่ 27 เมษายน ค.ศ. 2016 และมีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม ค.ศ. 2018

[5] Regulation (EU) 2016/679 (GDPR), Article 32

มาตรการลดความเสี่ยงดังกล่าวได้ คือ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ก่อนเริ่มต้นประมวลผลข้อมูลส่วนบุคคล[6]

สำหรับประเทศไทย ได้จัดทำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ[7] โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง[8] ดังนั้นจึงเห็นได้ว่าประเทศไทยมุ่งใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามระดับความเสี่ยงเช่นเดียวกับสหภาพยุโรป อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้องไม่ได้กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เช่นเดียวกับสหภาพยุโรป รวมถึงไม่ได้กำหนดแนวปฏิบัติเกี่ยวกับการทำ DPIA ไว้ ทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยยังขาดความชัดเจนในเรื่องหลักการประเมินความเสี่ยงและแนวทางการนำไปปฏิบัติที่เป็นรูปธรรมสำหรับองค์กรต่าง ๆ

บทความนี้จึงมุ่งศึกษาแนวทางการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยงของสหภาพยุโรป เพื่อนำมาจัดทำข้อเสนอแนะสำหรับการปรับปรุงกฎหมายและแนวปฏิบัติของประเทศไทยต่อไป

**ทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง**

Andreas Klinke และ Ortwin Renn (2002) เสนอกรอบแนวคิดสำหรับการจำแนกและจัดการความเสี่ยงที่ผสมผสานทั้งมิติทางวิทยาศาสตร์และสังคม และให้ความเห็นว่าความเสี่ยงแต่ละประเภทอาจมีกลยุทธ์การจัดการที่แตกต่างกัน สำหรับกลยุทธ์การจัดการตามหลักความเสี่ยง (Risk-Based) สามารถใช้ได้กับเหตุการณ์ที่มีความซับซ้อนสูงและมีข้อมูลเพียงพอ เช่น เขื่อนแตก (ความน่าจะเป็นต่ำ แต่ความเสียหายสูงมาก) เป็นต้น[9]

Yuhong Yan (2023) เห็นว่าแนวทางการกำกับดูแลตามระดับความเสี่ยง (Risk-based approach) เป็นเครื่องมือที่มีคุณค่าในการเสริมประสิทธิภาพการคุ้มครองข้อมูลส่วนบุคคล โดยช่วยให้การบังคับใช้กฎหมายมีความยืดหยุ่นและได้สัดส่วนมากขึ้น ทั้งในระดับชาติและระดับการค้าระหว่างประเทศ[10]

---

[6] Regulation (EU) 2016/679 (GDPR), Article 35

[7] มาตรา 37 (1) และ 40 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[8] ข้อ 4 (4) ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

[9] Klinke, A and Renn, O. (2002). *A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies*. Risk Analysis, Vol. 22, No. 6, 2002.

[10] Yan, Y. (2023). *The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law*. Beijing Law Review, 2023, 14, 1250-1270.

Raphael Gellert (2021) เห็นว่าแนวทางการกำกับดูแลตามระดับความเสี่ยงระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) และร่างกฎหมายปัญญาประดิษฐ์ (AI Act) ของสหภาพยุโรปมีความแตกต่างกัน โดยกฎหมาย GDPR ใช้ความเสี่ยงเป็นเครื่องมือช่วยให้สามารถปรับระดับมาตรการได้อย่างเหมาะสม ส่วน AI Act ใช้ความเสี่ยงเพื่อกำหนดว่าระบบ AI ใดควรถูกควบคุม[11]

Reuben Binns (2017) เห็นว่าระบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ในกฎหมาย GDPR ไม่ใช่การกำกับดูแลแบบใช้อำนาจบังคับทั่วไป แต่เน้นการผลักดันให้องค์กรดูแลตนเองโดยใช้กระบวนการภายใน ในขณะที่ยังคงถูกตรวจสอบจากภายนอก[12]

**วัตถุประสงค์**

1. เพื่อศึกษากฎหมายที่เกี่ยวข้องกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยงของสหภาพยุโรป
2. เพื่อศึกษาแนวปฏิบัติ และกรณีศึกษาการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของสหภาพยุโรป
3. เพื่อจัดทำข้อเสนอแนะแนวทางการปรับปรุงกฎหมายและแนวปฏิบัติของประเทศไทยเกี่ยวกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยนำแนวทางของสหภาพยุโรปมาประยุกต์ใช้

**ขอบเขตการวิจัย**

ศึกษาและวิเคราะห์กฎหมาย แนวปฏิบัติ และกรณีศึกษาที่เกี่ยวข้องกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง รวมถึงการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของสหภาพยุโรป เพื่อจัดทำข้อเสนอแนะแนวทางการปรับปรุงกฎหมายและแนวปฏิบัติของประเทศไทยเกี่ยวกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยนำแนวทางของสหภาพยุโรปมาประยุกต์ใช้

**วิธีดำเนินการวิจัย**

บทความนี้ใช้การวิจัยเชิงเอกสาร (Document Analysis) โดยศึกษาข้อมูลปฐมภูมิ ได้แก่ ตัวบทกฎหมาย แนวปฏิบัติ และกรณีศึกษาที่เกี่ยวข้อง รวมถึงข้อมูลทุติยภูมิจากเอกสารวิชาการ งานวิจัย หนังสือ

---

[11] Gellert, R. (2021). *The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?* Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021

[12] Binns, R. (2017). *Data protection impact assessments: a meta-regulatory approach*. International Data Privacy Law (2017) 7 (1): 22-35. Retrieved from https://doi.org/10.1093/idpl/ipw027

บทความ และข้อมูลที่เปิดเผยในเว็บไซต์ต่าง ๆ ที่เกี่ยวข้องกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยงของประเทศไทยและสหภาพยุโรป

**ผลการวิจัย**

**1. กฎหมายที่กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสหภาพยุโรป**

กฎหมายฉบับสำคัญที่กำหนดเรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสหภาพยุโรป ได้แก่ Regulation (EU) 2016/679 (GDPR)[13] ได้วางหลักการให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง (Risk-based approach) ทั้งนี้กฎหมาย GDPR ไม่ได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลแบบตายตัว แต่ให้พิจารณาตามระดับเทคโนโลยีในปัจจุบัน ต้นทุนในการดำเนินการ ลักษณะ ขอบเขต บริบทของการประมวลผล รวมถึงความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลต้องธำรงไว้ซึ่งความสามารถในการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) และความยืดหยุ่น (Resilience) ของระบบประมวลผลอย่างต่อเนื่อง[14] โดยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องใช้มาตรการทางเทคนิคและมาตรการเชิงองค์กรที่เหมาะสม เพื่อสร้างหลักประกันว่าระดับความมั่นคงปลอดภัยนั้นมีความเหมาะสมกับความเสี่ยง เช่น การทำข้อมูลแฝง (Pseudonymisation) การเข้ารหัสข้อมูล (Encryption) เป็นต้น[15]

ในการประเมินระดับความมั่นคงปลอดภัยที่เหมาะสม ให้คำนึงถึงความเสี่ยงที่เกิดจากการประมวลผลเป็นสำคัญ[16] หากการประมวลผลใดมีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ให้ผู้ควบคุมข้อมูลส่วนบุคคลประเมินผลกระทบของการประมวลผลที่มีต่อการคุ้มครองข้อมูลส่วนบุคคล[17] ก่อนการประมวลผลนั้น ซึ่งอย่างน้อยต้องมีรายละเอียด ได้แก่ คำอธิบายการประมวลผลและวัตถุประสงค์ของการประมวลผล การประเมินความจำเป็นและความได้สัดส่วนของการประมวลผลเมื่อเทียบกับวัตถุประสงค์ การประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลบุคคล และมาตรการจัดการกับความเสี่ยง รวมถึงมาตรการด้านความความปลอดภัยและกลไกเพื่อให้มั่นใจถึงการคุ้มครองข้อมูลส่วนบุคคล[18]

**2. แนวปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของสหภาพยุโรป**

---

[13] European Commission. (2026). *Legal framework of EU data protection*. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en#legislation

[14] Regulation (EU) 2016/679 (GDPR), Article 32 paragraph 1 (b)

[15] Regulation (EU) 2016/679 (GDPR), Article 32 paragraph 1 (a)

[16] Regulation (EU) 2016/679 (GDPR), Article 32 paragraph 2

[17] Regulation (EU) 2016/679 (GDPR), Article 35 paragraph 1

[18] Regulation (EU) 2016/679 (GDPR), Article 35 paragraph 7

คณะกรรมการคุ้มครองข้อมูลแห่งสหภาพยุโรปได้จัดทำ Guidelines on Data Protection Impact Assessment (DPIA) โดยกำหนดแนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ดังนี้[19]

**2.1 พิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นต้องทำ DPIA หรือไม่**

หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีลักษณะที่เข้าเกณฑ์ 2 ข้อขึ้นไป จากเกณฑ์ทั้งหมด 9 ข้อต่อไปนี้ ถือว่ามีความเสี่ยงสูงและต้องดำเนินการประเมินความเสี่ยงต่อไป

ข้อ 1 การประเมินหรือให้คะแนน รวมถึงการสร้างโปรไฟล์บุคคล เช่น สถาบันการเงินตรวจสอบข้อมูลลูกค้ากับฐานข้อมูลเครดิตบูโร บริษัทเทคโนโลยีชีวภาพเสนอบริการตรวจพันธุกรรมแก่ผู้บริโภคเพื่อประเมินความเสี่ยงด้านสุขภาพ บริษัทสร้างโปรไฟล์พฤติกรรมการตลาดจากการใช้งานเว็บไซต์

ข้อ 2 การตัดสินใจอัตโนมัติที่มีผลทางกฎหมายหรือส่งผลกระทบอย่างมีนัยสำคัญ เช่น การประมวลผลที่นำไปสู่การกีดกันหรือการเลือกปฏิบัติ

ข้อ 3 การเฝ้าติดตามอย่างเป็นระบบ เช่น การใช้กล้องวงจรปิดเพื่อเฝ้าระวังพื้นที่สาธารณะ

ข้อ 4 ข้อมูลอ่อนไหวหรือข้อมูลส่วนตัวอย่างมาก เช่น ความเห็นทางการเมือง ข้อมูลเกี่ยวกับประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลที่กระทบต่อการใช้สิทธิขั้นพื้นฐาน (ข้อมูลตำแหน่งที่ตั้ง) ข้อมูลที่หากรั่วไหลจะกระทบต่อการดำรงชีวิตอย่างรุนแรง (ข้อมูลทางการเงินที่อาจถูกนำไปฉ้อโกง)

ข้อ 5 การประมวลผลข้อมูลในปริมาณมาก โดยพิจารณาจากปัจจัยต่าง ๆ เช่น จำนวนเจ้าของข้อมูล ปริมาณข้อมูล ระยะเวลาในการประมวลผล ขอบเขตทางภูมิศาสตร์ของการประมวลผล

ข้อ 6 การจับคู่หรือการผสมผสานชุดข้อมูล เช่น การนำข้อมูลจาก 2 แหล่งขึ้นไป ที่จัดเก็บด้วยวัตถุประสงค์ต่างกัน หรือโดยผู้ควบคุมข้อมูลต่างรายกัน มาประมวลผลร่วมกันในลักษณะที่เกินความคาดหมายโดยชอบธรรมของเจ้าของข้อมูล

ข้อ 7 ข้อมูลของกลุ่มเปราะบาง เช่น เด็ก ลูกจ้าง ผู้ป่วยทางจิต ผู้แสวงหาที่พักพิง ผู้สูงอายุ คนไข้ หรือกรณีใด ๆ ที่พบว่ามีความเหลื่อมล้ำระหว่างสถานะของเจ้าของข้อมูลและผู้ควบคุมข้อมูล

ข้อ 8 การใช้เทคโนโลยีใหม่หรือนวัตกรรม เช่น การใช้ลายนิ้วมือร่วมกับการจดจำใบหน้าเพื่อควบคุมการเข้าออกอาคาร การใช้เทคโนโลยีใหม่ที่ความรู้ความเข้าใจในขณะนั้นยังจำกัดอาจก่อให้เกิดความเสี่ยงใหม่ ๆ ที่คาดไม่ถึงต่อสิทธิและเสรีภาพ (เช่น การใช้งาน Internet of Things ที่กระทบต่อความเป็นอยู่ส่วนตัว)

ข้อ 9 การประมวลผลที่ขัดขวางสิทธิการใช้บริการของเจ้าของข้อมูล เช่น ธนาคารตรวจสอบฐานข้อมูลเครดิตเพื่อตัดสินใจว่าจะอนุมัติเงินกู้หรือไม่

ตัวอย่างเช่น ในกรณีที่องค์กรต้องการนำ AI มาวิเคราะห์พฤติกรรมและประสิทธิภาพของพนักงาน 5,000 คนทั่วยุโรป โดยเก็บข้อมูลการเข้าออกงาน ผลการทำงาน และสุขภาพ ในกรณีดังกล่าวองค์กรต้องทำ DPIA เนื่องจากมีการเก็บข้อมูลสุขภาพของพนักงานอันเป็นการประมวลผลข้อมูลอ่อนไหว (ข้อ 4) และมีการใช้

[19] European Commission. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev.01).* Retrieved from https://ec.europa.eu/newsroom/article29/items/611236

AI ซึ่งเป็นเทคโนโลยีใหม่ (ข้อ 8) ดังนั้นกรณีดังกล่าวจึงมีลักษณะที่เข้าเกณฑ์ 2 ข้อ จาก 9 ข้อ ทำให้ต้องจัดทำ DPIA

**2.2 กำหนดผู้รับผิดชอบในการจัดทำ DPIA**

เป็นการกำหนดหน้าที่ให้ผู้รับผิดชอบในการจัดทำ DPIA เช่น ผู้ควบคุมข้อมูลส่วนบุคคลทำหน้าที่หลักในการจัดทำ DPIA เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทำหน้าที่ให้คำแนะนำและติดตามผล ผู้ประมวลผลข้อมูลส่วนบุคคลทำหน้าที่อำนวยความสะดวกในการจัดหาข้อมูลให้ผู้ควบคุมข้อมูลส่วนบุคคล

**2.3 จัดทำกระบวนการ DPIA ก่อนเริ่มประมวลผลข้อมูลส่วนบุคคล**

กระบวนการ DPIA เป็นวงจรต่อเนื่อง ประกอบด้วย 6 ขั้นตอนหลัก ได้แก่

ขั้นตอน 1 อธิบายการประมวลผล ได้แก่ ระบุวัตถุประสงค์ ประเภทข้อมูล ผู้รับข้อมูล ระยะเวลาเก็บและระบบที่เกี่ยวข้อง

ขั้นตอน 2 ประเมินความจำเป็นและสัดส่วน โดยตรวจสอบว่าเป็นการประมวลผลเท่าที่จำเป็น มีฐานทางกฎหมายที่ชัดเจน และเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล

ขั้นตอน 3 ระบุมาตรการที่มีอยู่ โดยรวบรวมมาตรการด้านความปลอดภัยและการปฏิบัติตามกฎหมายที่ดำเนินการอยู่แล้ว

ขั้นตอน 4 ประเมินความเสี่ยง โดยประเมินโอกาสที่จะเกิด (Likelihood) และความรุนแรง (Severity) เพื่อหาระดับความเสี่ยง (Risk level) ตัวอย่างเช่น กรณีที่องค์กรต้องการนำ AI มาวิเคราะห์พฤติกรรมและประสิทธิภาพของพนักงาน อาจมีประเด็นความเสี่ยงและระดับความเสี่ยง ได้แก่ (1) การใช้ AI จัดการเรื่องเลิกจ้างโดยอัตโนมัติ มีความเสี่ยงในระดับ “สูงมาก” (โอกาสเกิดสูง x ความรุนแรงสูงมาก) และ (2) ข้อมูลส่วนบุคคลของลูกค้ารั่วไหลไปยังคู่ค้าต่างประเทศ มีความเสี่ยงในระดับ “สูง” (โอกาสเกิดปานกลาง x ความรุนแรงสูง)

ขั้นตอน 5 กำหนดมาตรการจัดการความเสี่ยง โดยออกแบบมาตรการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ตัวอย่างเช่น (1) องค์กรอาจกำหนดมาตรการห้ามนำ AI มาใช้ตัดสินใจแต่เพียงผู้เดียว (ต้องมีมนุษย์คอยอนุมัติในขั้นตอนสุดท้าย) เพื่อช่วยลดความเสี่ยงในกรณีที่นำ AI มาใช้จัดการเรื่องเลิกจ้างโดยอัตโนมัติ ทำให้ความเสี่ยงลดลงจาก “สูงมาก” เป็น “สูง” (2) องค์กรอาจนำมาตรการเชิงเทคนิคโดยการทำข้อมูลแฝง (Pseudonymisation)[20] มาใช้ลดความเสี่ยงในกรณีที่ข้อมูลส่วนบุคคลของลูกค้ารั่วไหลไปยังคู่ค้าต่างประเทศ ทำให้ความเสี่ยงลดลงจาก “สูง” เป็น “ปานกลาง” เป็นต้น

ขั้นตอน 6 จัดทำเอกสารและทบทวน โดยบันทึกผลการประเมินและการตัดสินใจทั้งหมด และทบทวนเมื่อมีการเปลี่ยนแปลง

**2.4 ปรึกษาหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคล ในกรณีที่มีความจำเป็น**

หากความเสี่ยงที่เหลือยังคงสูงอยู่หลังจากกำหนดมาตรการจัดการความเสี่ยงแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องปรึกษาหน่วยงานกำกับดูแลก่อนเริ่มประมวลผล (Prior consultation)[21]

---

[20] หมายถึง กระบวนการจัดการข้อมูลส่วนบุคคลที่ทำให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้โดยตรง หากปราศจากการใช้ข้อมูลเพิ่มเติมอื่น ๆ มาประกอบ

[21] Regulation (EU) 2016/679 (GDPR), Article 36

**2.5 ทบทวนอย่างต่อเนื่อง**

การจัดทำ DPIA ต้องทบทวนซ้ำเมื่อมีเหตุการณ์สำคัญ เช่น การเปลี่ยนแปลงขอบเขตหรือวัตถุประสงค์การประมวลผล การนำเทคโนโลยีใหม่มาใช้ การเปลี่ยนแปลงบริบทขององค์กรหรือสังคม กรณีที่มีความเสี่ยงเพิ่มขึ้นหรือลดลงอย่างมีนัยสำคัญ เป็นต้น

**3. ตัวอย่างกรณีศึกษาการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของสหภาพยุโรป**

**กรณีศึกษาที่ 1 การประมวลผลข้อมูลชีวภาพเพื่อตรวจสอบการเข้าเรียนของนักเรียน**[22]

ในปี ค.ศ. 2019 หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลของสวีเดน (Swedish DPA) ได้สั่งปรับเทศบาลแห่งหนึ่งเป็นเงินจำนวน 200,000 โครนาสวีเดน (ประมาณ 20,000 ยูโร) เนื่องจากการใช้เทคโนโลยีจดจำใบหน้าเพื่อตรวจสอบการเข้าเรียนของนักเรียนในโรงเรียน โดยโรงเรียนไม่ได้จัดทำรายงานการประเมินผลกระทบ (DPIA) ที่เหมาะสม รวมถึงไม่ได้ดำเนินการขอคำปรึกษาล่วงหน้าจากหน่วยงานกำกับดูแล ทั้งนี้แม้โรงเรียนจะอ้างฐานการประมวลผลข้อมูลโดยอาศัยความยินยอม แต่ Swedish DPA เห็นว่าความยินยอมนั้นไม่สมบูรณ์ เมื่อพิจารณาจากความไม่สมดุลของอำนาจระหว่างเจ้าของข้อมูล (นักเรียน) และผู้ควบคุมข้อมูลส่วนบุคคล (โรงเรียน)

**กรณีศึกษาที่ 2 การใช้ซอฟต์แวร์ติดตามการทำงานของพนักงาน**[23]

ในปี ค.ศ. 2024 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส (CNIL) มีคำสั่งปรับบริษัทอสังหาริมทรัพย์แห่งหนึ่งจำนวน 40,000 ยูโร เนื่องจากบริษัทได้ใช้ซอฟต์แวร์ติดตามพฤติกรรมการเข้าชมเว็บไซต์และบันทึกหน้าจอการทำงานของพนักงาน ซึ่งถือเป็นการตรวจสอบพนักงานเข้มงวดเกินไป อันกระทบต่อสิทธิขั้นพื้นฐานและเสรีภาพของพนักงาน นอกจากนี้บริษัทไม่ได้จัดทำ DPIA เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยใช้ซอฟต์แวร์ติดตามการทำงานของพนักงาน ทั้งที่การประมวลผลดังกล่าวมีแนวโน้มสูงที่จะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของพนักงาน

**กรณีศึกษาที่ 3 การเก็บรวบรวมข้อมูลชีวภาพจำนวนมาก**[24]

ในปี ค.ศ. 2025 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส (CNIL) มีคำสั่งปรับบริษัทผู้ให้บริการระบบ AI จำนวน 20 ล้านยูโร และสั่งให้หยุดเก็บรวบรวมข้อมูลและลบข้อมูลของบุคคลในฝรั่งเศสจากการละเมิดหลายประการ เช่น การเก็บข้อมูลการจดจำใบหน้า (Facial recognition) ซึ่งเป็นข้อมูล

---

[22] European Data Protection Board. (2019). *Facial recognition in school renders Sweden's first GDPR fine.* Retrieved from https://www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

[23] Colin, R. (2025). *Employee monitoring at work: Regulatory enforcement actions against excessive employee monitoring practices continue.* Retrieved from https://www.arthurcox.com/knowledge/employee-monitoring-at-work-regulatory-enforcement-actions-against-excessive-employee-monitoring-practices-continue/

[24] Savulescu, S. (2025). *Artificial Intelligence and Data Protection: Call for Firm GDPR Enforcement in the Age of Algorithms.* Retrieved from https://www.legal500.com/developments/thought-leadership/artificial-intelligence-and-data-protection-call-for-firm-gdpr-enforcement-in-the-age-of-algorithms/

ชีวภาพจำนวนมากโดยไม่ขอความยินยอม เป็นต้น นอกจากนี้การประมวลผลข้อมูลชีวภาพดังกล่าวก็ไม่มีการจัดทำ DPIA ด้วย

**ประโยชน์ที่ได้รับ**

1) ทำให้เข้าใจถึงกฎหมายที่เกี่ยวข้องกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยงของสหภาพยุโรป

2) ทำให้เข้าใจถึงแนวปฏิบัติ และกรณีศึกษาการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ของสหภาพยุโรป

3) ข้อเสนอแนะแนวทางการปรับปรุงกฎหมายและแนวปฏิบัติของประเทศไทยเกี่ยวกับการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยนำแนวทางของสหภาพยุโรปมาประยุกต์ใช้

**สรุปและอภิปรายผล**

**สรุป**

ประเทศไทยและสหภาพยุโรปมีแนวทางในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่คล้ายคลึงกันหลายประการ เช่น การกำหนดมาตรการต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล มาตรการที่นำมาใช้อย่างน้อยต้องประกอบด้วยมาตรการเชิงเทคนิคและมาตรการเชิงองค์กร มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลไม่ได้ถูกกำหนดไว้แบบตายตัว การจัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลต้องเป็นมีความเหมาะสมตามระดับความเสี่ยง เป็นต้น

**อภิปรายผล**

แม้ว่าประเทศไทยกำหนดให้การจัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลต้องเป็นมีความเหมาะสมตามระดับความเสี่ยง แต่ไม่ได้กำหนดแนวทางการจัดทำมาตรการให้สอดคล้องกับระดับความเสี่ยงไว้ในกฎหมายลำดับรองหรือแนวปฏิบัติที่จัดทำโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในขณะที่สหภาพยุโรปกำหนดแนวทางการจัดทำมาตรการให้สอดคล้องกับความเสี่ยง ได้แก่ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ไว้ในกฎหมาย GDPR และแนวปฏิบัติ (Guideline) ที่จัดทำโดยคณะกรรมการคุ้มครองข้อมูลแห่งสหภาพยุโรป นอกจากนี้แนวปฏิบัติของสหภาพยุโรปได้กำหนดรายการ (Checklist) สำหรับการพิจารณาว่ากิจกรรมใดบ้างต้องจัดทำ DPIA เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำมาตรการลดความเสี่ยงโดยเฉพาะสำหรับกิจกรรมนั้น ทำให้ทำให้องค์กรเกิดต้นทุนในการจัดทำมาตรการลดความเสี่ยงเท่าที่จำเป็นและเหมาะสมกับระดับความเสี่ยง

เมื่อวิเคราะห์ถึงการจัดทำ DPIA ของสหภาพยุโรป พบว่ามีข้อดี ได้แก่ ทำให้องค์กรสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลได้เหมาะสมตามระดับความเสี่ยง ช่วยให้ผู้บริหารและทีมงานได้หยุดคิดถึงผลกระทบที่อาจเกิดขึ้นก่อนที่จะลงมือดำเนินการจริง เป็นหลักฐานชี้ให้เห็นถึงความ

รับผิดชอบขององค์กรที่นำไปแสดงต่อหน่วยงานกำกับดูแลได้ และในบางกรณีอาจช่วยลดความรับผิดทางกฎหมายได้ด้วย อย่างไรก็ตามการทำ DPIA ก็มีข้อเสีย ได้แก่ DPIA ทำให้เกิดภาระด้านเวลาและค่าใช้จ่ายแก่องค์กร หลายองค์กรจัดทำ DPIA เพื่อให้ครบตามข้อกำหนดทางกฎหมายเท่านั้นโดยไม่ได้มุ่งหวังผลลัพธ์ที่แท้จริง บางองค์กรยังสับสนระหว่าง DPIA กับการตรวจสอบภายใน บางองค์กรประเมินเฉพาะความเสี่ยงที่กระทบต่อองค์กรตนเอง เช่น ด้านชื่อเสียงหรือการเงิน โดยละเลยผลกระทบต่อบุคคลและสังคมในวงกว้าง นอกจากนี้ในบางครั้ง DPIA ถูกดำเนินการเมื่อโครงการออกแบบเสร็จสิ้นแล้ว ทำให้ผลการประเมินแทบไม่มีผลต่อการปรับแก้ไขกิจกรรมการประมวลผลใด ๆ อีก ดังนั้นจึงอาจสรุปได้ว่า DPIA เป็นเครื่องมือที่มีศักยภาพในการทำให้องค์กรสามารถกำหนดมาตรการได้เหมาะสมกับระดับความเสี่ยง แต่ประสิทธิผลที่แท้จริงขึ้นอยู่กับความจริงจังในการนำไปปฏิบัติ[25]

ทั้งนี้หากประเทศไทยนำแนวทางการทำ DPIA ของสหภาพยุโรปมาเป็นเครื่องมือช่วยกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคให้เหมาะสมตามระดับความเสี่ยง แม้ว่าจะช่วยให้การกำหนดมาตรการตามระดับความเสี่ยงเกิดความชัดเจน แต่ก็อาจเจอข้อเสียเช่นเดียวกับสหภาพยุโรป โดยเฉพาะในกรณีที่บางองค์กรจัดทำ DPIA เพื่อให้ครบตามข้อกำหนดทางกฎหมายโดยไม่ได้มุ่งหวังผลลัพธ์ที่แท้จริง ทำให้ DPIA ถูกนำมาใช้เป็นข้ออ้างว่าองค์กรได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมแล้ว

**ข้อเสนอแนะ**

จากที่กล่าวมาข้างต้น การทำ DPIA ตามแนวทางของสหภาพยุโรปมีทั้งข้อดีและข้อเสีย แต่ก็มีประโยชน์อย่างมากต่อองค์กรที่นำแนวทางดังกล่าวไปปฏิบัติอย่างจริงจัง ดังนั้นประเทศไทยจึงควรนำแนวทางการทำ DPIA ของสหภาพยุโรปมาใช้เป็นทางเลือกหนึ่งในข้อเสนอแนะของคู่มือการจัดทำมาตรการให้เหมาะสมกับความเสี่ยง โดยไม่จำเป็นต้องบัญญัติไว้ในกฎหมายเพื่อบังคับให้ปฏิบัติเช่นเดียวกับสหภาพยุโรป ทั้งนี้เพื่อให้องค์กรที่มีความพร้อมหรือมีความจริงจังในการนำไปปฏิบัติสามารถนำแนวทางดังกล่าวไปใช้ประโยชน์ได้ต่อไป

ผู้เขียนเห็นว่าควรนำแนวทางการทำ DPIA ของสหภาพยุโรปมาประยุกต์ใช้กับประเทศไทย เพื่อให้การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยงของประเทศไทยมีแนวทางที่ชัดเจนมากขึ้น ดังนี้

1. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ควรจัดทำ “คู่มือการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” เพื่อแนะนำแนวทางในการจัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้สอดคล้องกับระดับความเสี่ยง (Risk-Based Approach) รวมถึงแนะนำให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่

[25] Kloza, D., Van Djik, N., Gillert, R., BÖRÖCZ, I., Tanas, A., Mantovani, E. & Quinn, P. (2017). *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals*. d.pia.lab Policy Brief No. 1/2017, 2-3.

มีแนวโน้มว่าจะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยกำหนดขั้นตอนเช่นเดียวกับสหภาพยุโรป ได้แก่

(1) พิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้นต้องทำ DPIA หรือไม่

(2) กำหนดผู้รับผิดชอบในการจัดทำ DPIA

(3) จัดทำกระบวนการ DPIA ก่อนเริ่มเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(4) ปรึกษาหน่วยงานกำกับดูแลด้านข้อมูลส่วนบุคคล ในกรณีที่มีความจำเป็น

(5) ทบทวนอย่างต่อเนื่อง

การกำหนดแนวทางการจัดทำ DPIA ในแนวปฏิบัติหรือคู่มือ ทำให้เกิดความชัดเจนว่าควรใช้เครื่องมือใดในการจัดทำมาตรการรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง และช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลมีแนวทางที่น่าเชื่อถือในการนำไปปฏิบัติได้อย่างเป็นรูปธรรม

2. คู่มือที่จัดทำโดย สคส. ควรกำหนดรายการ (Checklist) พร้อมตัวอย่างประกอบ สำหรับการพิจารณาว่ากรณีใดบ้างต้องจัดทำ DPIA เช่นเดียวกับสหภาพยุโรป (เข้าเกณฑ์ 2 ข้อขึ้นไป ต้องทำ DPIA) เช่น การสร้างโปรไฟล์บุคคล การตัดสินใจอัตโนมัติที่มีผลทางกฎหมาย การประมวลผลข้อมูลที่อ่อนไหว การประมวลผลข้อมูลในปริมาณมาก เป็นต้น ทั้งนี้การจัดทำ Checklist พร้อมตัวอย่างประกอบย่อมช่วยให้องค์กรต่าง ๆ สามารถทำความเข้าใจคู่มือได้ง่าย โดยเฉพาะในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นองค์กรขนาดเล็กที่มีกิจกรรมการประมวลผลส่วนใหญ่ไม่เข้าข่ายที่จะต้องทำ DPIA หากองค์กรพิจารณาตาม Checklist แล้วว่ากิจกรรมนั้นไม่มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรก็ไม่ต้องจัดทำ DPIA และไม่ต้องกำหนดมาตรการลดความเสี่ยงสำหรับกิจกรรมนั้นเป็นพิเศษ ทำให้องค์กรมีต้นทุนในการจัดทำมาตรการลดความเสี่ยงเท่าที่จำเป็นและเหมาะสมกับระดับความเสี่ยง

**บรรณานุกรม**

Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. International Data Privacy Law (2017) 7 (1): 22-35. Retrieved from https://doi.org/10.1093/idpl/ipw027

Colin, R. (2025). Employee monitoring at work: Regulatory enforcement actions against excessive employee monitoring practices continue. Retrieved from https://www.arthurcox.com/knowledge/employee-monitoring-at-work-regulatory-enforcement-actions-against-excessive-employee-monitoring-practices-continue/

European Commission. (2026). Legal framework of EU data protection. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en#legislation

European Commission. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of

Regulation 2016/679 (WP 248 rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/items/611236

European Data Protection Board. (2019). Facial recognition in school renders Sweden's first GDPR fine. Retrieved from https://www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

Gellert, R. (2021). The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021

Klinke, A and Renn, O. (2002). A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. Risk Analysis, Vol. 22, No. 6, 2002.

Kloza, D., Van Djik, N., Gillert, R., BÖRÖCZ, I., Tanas, A., Mantovani, E. & Quinn, P. (2017). Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. d.pia.lab Policy Brief No. 1/2017.

Savulescu, S. (2025). Artificial Intelligence and Data Protection: Call for Firm GDPR Enforcement in the Age of Algorithms. Retrieved from https://www.legal500.com/developments/thought-leadership/artificial-intelligence-and-data-protection-call-for-firm-gdpr-enforcement-in-the-age-of-algorithms/

Yan, Y. (2023). The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law. Beijing Law Review, 2023, 14, 1250-1270.