รูปแบบการวิจัยทางสังคมศาสตร์เพื่อค้นหาแนวทางให้บริษัทเอกชนปฏิบัติตามไม่ละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Social Science Research Methods to Find Approaches for Private Sector Organizations to Comply With and Not Violate The Personal Data Protection Act B.E. 2562

อภิญญา ทักศินาวรรณ[1], บรรพต วิรุณราช[1], รดา วงศ์เลิศคุณากร[2],
มนสิชา โพธิสุข[1] และนภาวรรณ ลับบัวงาม[1]
[1]มหาวิทยาลัยนอร์ทกรุงเทพ และ [2]มหาวิทยาลัยหอการค้าไทย
Aphinya Taksinawan[1], Banpot Wiroonratch[1], Rhada Wonglertkunakorn[2],
Monsicha Potisook[1] and Napawan Labbuangam[1]
[1] North Bangkok University, [2] University of the Thai Chamber of Commerce

ประวัติย่อ

1. นางสาวอภิญญา ทักศินาวรรณ (Corresponding author) พนักงานบริษัทฯ และนักศึกษาหลักสูตรปริญญาเอก สาขารัฐประศาสนศาสตร์ คณะรัฐศาสตร์ มหาวิทยาลัยนอร์ทกรุงเทพ e-mail: Aphinya_apo@hotmail.com เชี่ยวชาญ ด้านการบริหารและพัฒนาทรัพยากรมนุษย์

2. รองศาสตราจารย์ ดร.บรรพต วิรุณราช อาจารย์ คณะรัฐศาสตร์ มหาวิทยาลัยนอร์ทกรุงเทพ e-mail: banpot.buu@gmail.com ความเชี่ยวชาญ ด้านรัฐศาสตร์ และด้านรัฐประศาสนศาสตร์

3. ดร.รดา วงศ์เลิศคุณากร อาจารย์ คณะบริหารธุรกิจ มหาวิทยาลัยหอการค้าไทย e-mail: rhada_won@utcc.ac.th ความเชี่ยวชาญ ด้านบริหารธุรกิจ

4. นางมนสิชา โพธิสุข อาจารย์ สาขารัฐศาสตร์ คณะรัฐศาสตร์ มหาวิทยาลัยนอร์ทกรุงเทพ e-mail: monsicha.po@northbkk.ac.th ความเชี่ยวชาญ ด้านกฎหมายอาญา และกฎหมายแพ่ง

5. นางสาวนภาวรรณ ลับบัวงาม อาจารย์ คณะรัฐศาสตร์ มหาวิทยาลัยนอร์ทกรุงเทพ e-mail: napawan.la@northbkk.ac.th ความเชี่ยวชาญ ด้านกฎหมายแพ่ง

Revised: September 4, 2024; Revised: October 4, 2024; Accepted: October 15, 2024

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์ เพื่อศึกษารูปแบบงานวิจัย ที่จะทำให้ค้นพบวิธีการปฏิบัติของบริษัทเอกชนที่ไม่ละเมิดกฎหมาย PDPA เป็นการวิจัยเชิงคุณภาพ มี 2 ขั้นตอน คือ สัมภาษณ์กลุ่มผู้ให้ข้อมูลหลัก 6 คน เป็นอาจารย์สอนวิจัย และสนทนากลุ่ม 6 คน กับผู้บริหารทรัพยากรมนุษย์ 6 บริษัท ๆ ละ 1 คน เลือกแบบเจาะจง ผลการวิจัยพบว่า รูปแบบการวิจัยทางสังคมศาสตร์ที่เหมาะสม ที่จะหาแนวทางการปฏิบัติให้บริษัทเอกชน ในการไม่ละเมิดกฎหมาย PDPA ได้แก่ วิจัย R and D (วิจัยและพัฒนา) ด้วยเหตุผลที่ว่า เป็นการค้นหาและพัฒนาทดลองจริงมาแล้วก่อนเผยแพร่ให้มีการปฏิบัติ

คำสำคัญ: กฎหมาย PDPA, การคุ้มครอง, ข้อมูลส่วนบุคคล, R and D, บริษัทเอกชน

Abstract

This research aims to study research methods that will lead to discovering practices for Private Sector Organizations to comply with the PDPA law without violating it. It is a qualitative research study consisting of two stages: interviewing a group of 6 key informants who are research instructors and conducting a focus group discussion with 6 Human Resource Managers from 6 companies, with 7 participants from each company, selected through purposive sampling. The research findings reveal that the appropriate social science research method to find practical approaches for Private Sector Organizations to avoid violating the PDPA law is R&D (Research and Development). The rationale is that this method involves discovering, developing, and testing practices before disseminating them for implementation.

Keywords: PDPA, Protection, Personal Data, R and D, Private Sector Organizations

บทนำ

ด้วยความเจริญก้าวหน้าทางด้านเทคโนโลยีในโลกปัจจุบัน รวมทั้งระบบการสื่อสารที่ได้มีการพัฒนาไปอย่างรวดเร็ว ทำให้การเข้าถึง การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล ทำได้โดยง่าย สะดวกและรวดเร็ว ซึ่งอาจนำความเสียหายต่อเจ้าของข้อมูล กอปรกับประเทศไทย ได้มีการประกาศพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 ซึ่งเป็นกฎหมายที่ตราขึ้นมา เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งาน ไปจนถึงการส่งเสริมเศรษฐกิจระหว่างประเทศ เพื่อให้ได้รับการยอมรับในระดับสากล โดยที่องค์กรต่าง ๆ ที่มีการเก็บข้อมูลส่วนบุคคลจะต้องไม่นำข้อมูลเหล่านั้นไปเปิดเผยหรือใช้ในกิจกรรมต่าง ๆ หากเจ้าของข้อมูลไม่ให้ความยินยอม หรือที่กฎหมายยกเว้นให้ทำได้โดยไม่ต้องขอความยินยอม (ออพติมุส, 2564) รวมถึงหลักปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ซึ่งบุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิ หรือการลบหลู่ดังกล่าวนั้น (กรมองค์การระหว่างประเทศ, 2551)

เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เริ่มบังคับใช้อย่างเต็มรูปแบบ เจ้าของธุรกิจและฝ่ายบริหารงานทรัพยากรบุคคล จะต้องให้ความสำคัญในเรื่องนี้เป็นอย่างมาก เนื่องจากข้อมูลของพนักงานนั้น ถือเป็นข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ PDPA โดยตรง ซึ่งบทบาทของนายจ้างและฝ่ายบริหารงานทรัพยากรบุคคล นอกจากจะต้องศึกษาและทำความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ดีแล้ว ยังจะต้องรู้ถึงวิธีการป้องกัน เพื่อไม่ให้เกิดปัญหาขึ้นในอนาคต (PDPA Pro, 2563)

อย่างไรก็ตามปี พ.ศ.2565 หลังกฎหมาย PDPA มีผลบังคับใช้มา 3 ปี พบว่า ยังมีความไม่เข้าใจในการปฏิบัติ ซึ่งสภาองค์กรของผู้บริโภค (2565) ได้ประมวลจากกลุ่มผู้บริโภค และสรุปว่ามีผู้ประกอบการบังคับให้คนงาน ยินยอมให้เก็บข้อมูลก่อนแล้วไปยกเลิกภายหลัง และพบว่าภาคเอกชนเป็นองค์กรที่มีโอกาสละเมิดกฎหมายนี้มากที่สุด โดยที่หากกระทำผิดตามกฎหมาย PDPA จะมีบทลงโทษหนัก ได้แก่ โทษทางอาญา จำคุกสูงสุดไม่เกิน 6 เดือน ถึง 1 ปี หรือปรับสูงสุดไม่เกิน 500,000 บาท ถึง 1,000,000 ล้าน หรือทั้งจำทั้งปรับ

ดังนั้น จากประเด็นที่พบว่า บริษัทเอกชนมีโอกาสละเมิดกฎหมาย PDPA สูง และบทลงโทษการละเมิดสูง จึงเป็นเหตุที่บริษัทเอกชนจะต้องสนใจว่า จะมีวิธีการปฏิบัติอย่างไรให้ลดหรือไม่มีการละเมิดกฎหมาย PDPA นี้ โดยในเชิงวิชาการจักต้องทำวิจัยรูปแบบใด เพื่อแสดงหาข้อสรุปถึงวิธีการสร้างรูปแบบการปฏิบัติที่ไม่ละเมิดกฎหมาย PDPA นี้

วัตถุประสงค์

เพื่อศึกษารูปแบบงานวิจัยที่จะทำให้ค้นพบวิธีการปฏิบัติของบริษัทเอกชน ที่ไม่ละเมิดกฎหมาย PDPA

ประโยชน์ที่ได้รับ

1. ได้ข้อมูลแจ้งสถานศึกษาที่มีนักวิจัย ถึงประเด็นการวิจัยและรูปแบบการวิจัย ที่จะได้แนวทางเป็นประโยชน์ต่อภาคเอกชน ในเรื่องการปฏิบัติตามกฎหมาย PDPA
2. ได้ข้อมูลที่ผู้บริหารบริษัทเอกชน บุคลากรจะร่วมมือกับนักวิจัยในการค้นหาวิธีการ รูปแบบการ

ทบทวนวรรณกรรม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายหลักของประเทศไทยที่กำหนดหลักเกณฑ์ กลไก และมาตรการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยมีผลบังคับใช้อย่างเต็มรูปแบบตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2565)

General Data Protection Regulation (GDPR)

General Data Protection Regulation เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ที่มีผลบังคับใช้ในเดือนพฤษภาคม ปี พ.ศ. 2561 และมีอิทธิพลต่อการออกแบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศทั่วโลก รวมถึงประเทศไทย โดยมีวัตถุประสงค์เพื่อให้ประชาชน มีสิทธิควบคุมข้อมูลส่วนบุคคลของตน ซึ่งถือเป็นสิทธิขั้นพื้นฐาน (สถาบันวิชาการนโยบายกิจการสาธารณะกับธุรกิจ และการกำกับดูแล, 2561) GDPR มีสาระสำคัญ คือ องค์กรธุรกิจที่จำเป็นต้องจัดเก็บและจัดการข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป จะต้องเพิ่มมาตรการปกป้องข้อมูลต่าง ๆ ซึ่งข้อมูลเหล่านี้ จะไม่สามารถนำไปใช้ในเชิงพาณิชย์ได้ หากไม่ได้รับความยินยอมจากเจ้าของข้อมูล การละเมิดกฎระเบียบนี้อาจถูกปรับเป็นจำนวนเงินค่อนข้างสูง GDPR มีผลบังคับใช้ปกป้องข้อมูลพลเมืองสหภาพยุโรป ไม่ว่าจะอยู่ที่ใดในโลกนี้ และแม้ว่าบริษัทธุรกิจดังกล่าว จะไม่ได้ตั้งอยู่ในสหภาพยุโรปก็ตาม (กรมการค้าต่างประเทศ, 2024)

ISO/ IEC 27701:2019

มาตรฐาน ISO/ IEC 27701: 2019 เป็นมาตรฐานระบบการจัดการความเป็นส่วนตัวของข้อมูล (Privacy Information Management System: PIMS) ที่ขยายมาจากมาตรฐาน ISO/IEC 27001 และ ISO/ IEC 27002 โดยให้แนวทางในการบริหารจัดการความเป็นส่วนตัวของข้อมูลในองค์กร หลักปฏิบัติสำหรับการควบคุมความปลอดภัยของข้อมูล ในมาตรฐาน ISO/IEC 27701 ถูกประกาศใช้และยอมรับไปทั่วโลก โดยให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึง วิธีที่องค์กรควรบริหารจัดการข้อมูลส่วนบุคคล และแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดการคุ้มครองข้อมูลส่วนบุคคล (The British Standards Institution, 2024)

ISACA Privacy Principles

ISACA Privacy Principles คือ หลักการด้านความเป็นส่วนตัวที่กำหนดโดย ISACA (Information Systems Audit and Control Association) ซึ่งเป็นองค์กรระดับโลกที่เชี่ยวชาญด้านการกำกับดูแลเทคโนโลยีสารสนเทศ หลักการเหล่านี้ถูกออกแบบมา เพื่อเป็นแนวทางสำหรับองค์กรในการจัดการและปกป้องข้อมูลส่วนบุคคล โดยครอบคลุมประเด็นสำคัญต่าง ๆ เช่น ทางเลือกและความยินยอม ข้อกำหนดวัตถุประสงค์ที่ถูกต้องตามกฎหมายและข้อจำกัดการใช้งาน วงจรชีวิตข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน ความแม่นยำและคุณภาพ การเปิดกว้าง ความโปร่งใส และการแจ้งให้ทราบ การมีส่วนร่วมส่วนบุคคล ความรับผิดชอบ มาตรการรักษาความปลอดภัย การติดตาม การวัด และการรายงาน การป้องกันอันตราย การจัดการบุคคลที่สาม/ผู้ขาย การจัดการการละเมิด ความปลอดภัยและความเป็นส่วนตัวโดยการออกแบบ และการไหลของข้อมูลอย่างเสรีและข้อจำกัดทางกฎหมาย หลักการต่าง ๆ เหล่านี้ช่วยให้องค์กรสามารถสร้างและรักษานโยบายความเป็นส่วนตัวที่มีประสิทธิภาพ ซึ่งสอดคล้องกับกฎหมายและมาตรฐานสากล (Rebecca Herold, 2017)

NIST Privacy Framework

NIST Privacy Framework คือ กรอบการทำงานที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (National Institute of Standards and Technology - NIST) เพื่อช่วยองค์กรในการจัดการความเสี่ยงด้านความเป็นส่วนตัว และการคุ้มครองข้อมูลส่วนบุคคล โดยมีจุดประสงค์หลัก ในการสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย เกี่ยวกับการจัดการข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ และรับผิดชอบ กรอบการทำงานนี้ ประกอบด้วยฟังก์ชั่นหลัก 5 ประการ: ระบุ (Identify) ควบคุม (Govern) ควบคุม (Control) สื่อสาร (Communicate) และป้องกัน (Protect) แต่ละฟังก์ชั่นมีหมวดหมู่และการควบคุม

ที่เฉพาะเจาะจง เพื่อช่วยองค์กรในการจัดการความเสี่ยงด้านความเป็นส่วนตัว (National institute of standards and technology, 2024)

การกำหนดนโยบายและแนวปฏิบัติด้านข้อมูลส่วนบุคคล

องค์กรควรจัดทำนโยบายและแนวปฏิบัติด้านข้อมูลส่วนบุคคลที่ชัดเจน ครอบคลุมประเด็นสำคัญ เช่น วัตถุประสงค์ในการเก็บรวบรวมข้อมูล การใช้และเปิดเผยข้อมูล มาตรการรักษาความปลอดภัย และสิทธิของเจ้าของข้อมูล (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2565) อีกทั้ง ปิยธิดา ดวดขุนทด และคณะ (2566) มีข้อเสนอแนะว่า นอกจากองค์กรควรจะจัดทำนโยบายให้สอดคล้องกับเจตจำนงของพระราชบัญญัติฯ แล้ว องค์กรควรกำหนดบทบาทหน้าที่ผู้รับผิดชอบ และคุณสมบัติของผู้ปฏิบัติงานอย่างเหมาะสม รวมถึงควรมีการกำหนดวิธีการดำเนินงานที่มีประสิทธิภาพ ในการป้องกันคุ้มครองข้อมูลส่วนบุคคลได้จริง และควรจัดให้มีการสื่อสารที่ครอบคลุมทั่วถึง เพื่อให้เกิดความเข้าใจที่ถูกต้องเป็นแนวทางเดียวกันทั้งองค์กร

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (2565) ได้เสนอแนวทางในการกำหนดนโยบายและกรอบการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล สำหรับองค์กรภาคเอกชน โดยเน้นย้ำความสำคัญของการมีนโยบายที่ชัดเจน และสอดคล้องกับกฎหมายในระดับสากล Voigt and von dem Bussche (2021) ได้วิเคราะห์แนวทางการปฏิบัติตาม GDPR สำหรับองค์กรธุรกิจ โดยเสนอให้มีการจัดทำ Data Protection Impact Assessment (DPIA) เพื่อประเมินความเสี่ยงและผลกระทบ ที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล

การขอความยินยอมจากเจ้าของข้อมูล

การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดแจ้ง โดยแจ้งวัตถุประสงค์และรายละเอียดการใช้ข้อมูลให้ทราบก่อน (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 19) โดยลักษณะของการขอความยินยอมจากเจ้าของข้อมูล สอดคล้องกับการศึกษาของ กมลวรรณ ตันติพิวัฒนสกุล และคณะ (2565) “ขั้นตอนการให้บริการเภสัชกรรมทางไกล ที่ต้องปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล ควรแจ้งข้อมูลผู้ให้บริการ และแจ้งวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลแก่ผู้มารับบริการทุกครั้ง โดยมีการแจ้งผ่านช่องทางต่าง ๆ ที่ทั้งผู้ให้บริการ และผู้รับบริการสะดวก เช่น การแจ้งผ่านหนังสือขอความยินยอม หรือแอพลิเคชั่น”

การรักษาความมั่นคงปลอดภัยของข้อมูล

องค์กรต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม ทั้งด้านเทคนิคและการบริหารจัดการ เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ (ธนาคารแห่งประเทศไทย, 2565) และต้องจัดเก็บรักษาข้อมูลไว้ ได้ตามระยะเวลาที่กำหนด หรือเท่าที่จำเป็น เพื่อให้บรรลุวัตถุประสงค์ตามที่ได้แจ้งต่อเจ้าของข้อมูล เว้นแต่ บุคคลที่เกี่ยวข้องกับข้อมูลได้ให้ความยินยอมอย่างชัดแจ้งว่า ให้เก็บรักษาข้อมูลนั้นเกินกว่าระยะเวลาตามที่กำหนดได้ กรณีจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคล ที่อยู่ในความควบคุมดูแลให้แก่บุคคลอื่น ต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน เว้นแต่ กรณีจำเป็นเร่งด่วนเกี่ยวกับประโยชน์ของส่วนรวม หรือกรณีที่อาจก่อให้เกิดความเสียหายแก่ชีวิต ร่างกายหรืออนามัยของบุคคล จะต้องแจ้งให้เจ้าของข้อมูลทราบโดยเร็วภายใน 15 วัน นับแต่วันส่งหรือโอนข้อมูลนั้น (เธียรชัย, 2565)

ธนาคารแห่งประเทศไทย (2565) ได้ออกแนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยเน้นการใช้เทคโนโลยีการเข้ารหัสข้อมูล และการควบคุมการเข้าถึงข้อมูลสอดคล้องกับ National Institute of Standards and Technology (2023) ที่เสนอแนวทางการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลส่วนบุคคล โดยใช้กรอบการทำงาน Privacy Framework

การจัดการสิทธิของเจ้าของข้อมูล

องค์กรต้องจัดให้มีช่องทางและกระบวนการ ในการรับคำร้องขอใช้สิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึงข้อมูล การแก้ไขข้อมูล การลบข้อมูล และการคัดค้านการประมวลผลข้อมูล (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2564) สอดคล้องกับ วันพิชิต ชินตระกูลชัย. (2021) ที่ระบุว่า ต้องจัดทำช่องทางสำหรับเจ้าของข้อมูลในการใช้สิทธิตามที่กฎหมายกำหนด สามารถให้ตรวจสอบยืนยันตัวตน ตรวจสอบความถูกต้องของคำขอ ดำเนินการตามสิทธิที่เจ้าของข้อมูลส่วนบุคคลร้องขอ และการแจ้งผลการดำเนินการ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2564) ได้นำเสนอแนวทางในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูล รวมถึงการจัดทำระบบและกระบวนการ เพื่อรองรับการใช้สิทธิตามกฎหมาย Information Commissioner's Office (2022) ได้ให้แนวทางเชิงปฏิบัติในการจัดการสิทธิของเจ้าของข้อมูลตาม GDPR โดยเน้นความโปร่งใส และการตอบสนองต่อคำขอของเจ้าของข้อมูลอย่างทันท่วงที

การจัดการกรณีละเมิดข้อมูล

European Data Protection Board (2023) ได้ออกแนวทางการแจ้งเตือน กรณีเกิดการละเมิดข้อมูลส่วนบุคคล โดยระบุขั้นตอนและระยะเวลาในการแจ้งเตือนหน่วยงานกำกับดูแล และผู้ได้รับผลกระทบ Kuner (2020) ได้วิเคราะห์แนวปฏิบัติในการจัดการกรณี จากการทบทวนวรรณกรรม พบว่า แนวทางการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคลในองค์กรภาคเอกชน มีความซับซ้อนและต้องอาศัยการบูรณาการหลายมิติ ทั้งด้านกฎหมาย เทคโนโลยี และการบริหารจัดการองค์กร การปฏิบัติตามแนวทางเหล่านี้ จะช่วยให้องค์กร สามารถคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ และสอดคล้องกับกฎหมาย

การฝึกอบรมและสร้างความตระหนัก

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (2565) ได้เสนอแนวทางการฝึกอบรมพนักงาน เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยเน้นการสร้างความตระหนักและการปรับเปลี่ยนพฤติกรรมในการจัดการข้อมูล Solove and Schwartz (2022) ได้เน้นย้ำความสำคัญของการสร้างวัฒนธรรมองค์กร ที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล โดยเสนอแนวทางการฝึกอบรม ที่เน้นการเรียนรู้จากกรณีศึกษา และการฝึกปฏิบัติจริง

แนวทางการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล ในองค์กรภาคเอกชน

ปิยธิดา ดวดขุนทด และคณะ (2566) เสนอแนวทางการบริหารจัดการคุ้มครองข้อมูลส่วนบุคคล ในองค์กรภาคเอกชน ไว้ดังนี้ 1) องค์กรควรทำความเข้าใจในเจตจำนง ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และให้ความสำคัญของการปฏิบัติตามพระราชบัญญัติอย่างจริงจัง ซึ่งจะส่งผลดีทั้งในแง่ของการปฏิบัติตามกฎหมาย การได้รับการยอมรับจากทั้งบุคคลภายในและนอกองค์กร รวมถึง ยังเป็นการป้องกันการรั่วไหลและละเมิดสิทธิส่วนบุคคล ทั้งนี้ ผู้บริหารต้องให้ความสำคัญ ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลเป็นหลัก โดยสอดคล้องกับ เธียรชัย (2565) ซึ่งกล่าวว่า “การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่ดี มีประสิทธิภาพจำเป็นที่ผู้บริหารองค์กร ควรมีแนวปฏิบัติที่เป็นมาตรฐานสากลในระดับประเทศและระหว่างประเทศ” และจัดให้มีการศึกษาใจความสำคัญของพระราชบัญญัติ ทั้งเรื่องการขอความยินยอมจากเจ้าของข้อมูล การเก็บรวบรวมข้อมูลส่วนบุคคล การใช้และเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล ก่อนที่จะออกนโยบายเพื่อใช้ในองค์กร 2) ต้องมีการตรวจสอบนโยบาย ให้มีความสอดคล้องกับพระราชบัญญัติฯ ทั้งเรื่องการขอความยินยอมจากเจ้าของข้อมูล การเก็บรวบรวมข้อมูลส่วนบุคคล การใช้และเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล ก่อนจะนำไปออกแบบเป็นขั้นตอนการปฏิบัติงาน โดยมีการให้ความรู้ที่ถูกต้องกับคณะผู้ดำเนินการเชิงนโยบาย อันได้แก่ พนักงานทั่วไป พนักงานระดับบริหาร พนักงานระดับผู้จัดการและฝ่ายกฎหมาย 3) ผู้ที่รับผิดชอบด้านการดำเนินงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ต้องมีคุณสมบัติและลักษณะงานที่เหมาะสม เป็นผู้มีความเข้าใจในพระราชบัญญัติฯ และมีการตระหนักถึงผลลัพธ์ที่จะเกิดขึ้น หากมีกรณีข้อมูลส่วนบุคคลถูกล่วงละเมิด ซึ่งจะทำให้เกิดความเสียหายแก่เจ้าของข้อมูลและนำพาความเสียหายมาสู่องค์กรได้ และ 4) ควรสื่อสารให้เกิดความเข้าใจในนโยบายและวิธีการปฏิบัติงานให้สอดคล้องกับนโยบาย หากผู้ปฏิบัติงาน หรือผู้เกี่ยวข้อง ตลอดจนเจ้าของข้อมูลไม่ได้รับการสื่อสารที่ถูกต้องและดีเพียงพอ จะทำให้เกิดความเข้าใจผิดพลาด สอดคล้องกับ สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (2565) ที่ระบุว่า “องค์กรควรจัดให้มีการฝึกอบรมพนักงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เพื่อสร้างความตระหนักและความเข้าใจในการปฏิบัติตามกฎหมายและนโยบายขององค์กร

เธียรชัย (2565) ได้นำเสนอแนวทางปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคล ในองค์กรภาคเอกชนออกเป็น 3 แนวทาง ดังนี้ 1) แนวทางปฏิบัติสำหรับผู้บริหารองค์กร: ผู้บริหารองค์กรควรมีแนวปฏิบัติที่เป็นมาตรฐานสากลในระดับประเทศและระหว่างประเทศ 2) แนวทางปฏิบัติเชิงนโยบายที่ต้องประกาศให้สาธารณชนได้ทราบ ซึ่งจะเน้นหลักเกณฑ์ที่เป็นมาตรฐานขั้นต่ำ ที่องค์กรธุรกิจควรเปิดเผยสู่สาธารณชน เพื่อสร้างความมั่นใจแก่ลูกค้าหรือผู้ใช้บริการ ในระบบการจัดเก็บข้อมูลส่วนบุคคลขององค์กรนั้น ๆ และ 3) แนวทางภายในองค์กรภาคเอกชน ซึ่งควรจัดทำหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล ขึ้นใช้ภายในองค์กร เพื่อเป็นแนวทางปฏิบัติสำหรับพนักงานหรือเจ้าหน้าที่ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล สามารถนำไปปฏิบัติได้อย่างถูกต้อง

จากวรรณกรรมทั้งหมดที่กล่าวมา พบว่า ก่อนเกิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกาศใช้ ในต่างประเทศมีการคำนึงถึงเรื่องสิทธิส่วนบุคคล ข้อมูลส่วนบุคคลมานานแล้ว จึงมาถึงประเทศไทย ที่จำเป็นต้องแสดงให้ทุกประเทศเห็นว่า ประเทศไทยมีกฎหมายเช่นเดียวกัน ซึ่งการออกกฎหมายในลักษณะพระราชบัญญัติ จัดว่าเป็นกฎหมายขั้นสูงรองจากรัฐธรรมนูญ และมีการวิจัยที่เสนอว่า ควรเร่งให้มีการให้ความรู้ประชาชนไทย ถึงเรื่องความเข้าใจในกฎหมาย PDPA นี้ โดยการฝึกอบรม สำหรับบริษัทเอกชน สิ่งที่จะปฏิบัติได้ถูก สิ่งที่จะอบรมควรค้นพบเนื้อหาที่จะอบรมจากงานวิจัย การวิจัยมีหลายประเภท และหลายวิธีการ จึงต้องค้นหาวิธีการวิจัยว่าวิธีการใดเหมาะสม

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยมีขั้นตอนการวิจัย 2 ขั้นตอน สัมภาษณ์อาจารย์ที่สอนด้านวิจัย 6 คน และนำผลสรุปที่ได้ จัดสนทนากลุ่มกับผู้บริหารบริษัทเอกชน ที่ทำงานด้านทรัพยากรมนุษย์ 6 บริษัท (Morse, 1994) บริษัทละ 1 คน โดยการเลือกแบบเจาะจง ทั้งนี้มีคำถามเพื่อนำไปสัมภาษณ์เป็นกึ่งโครงสร้าง ได้แก่ ในฐานะที่ท่านเป็นอาจารย์สอนด้านวิจัย ท่านคิดว่าการที่บริษัทเอกชนจะปฏิบัติตามกฎหมาย PDPA ควรปฏิบัติอย่างไร การค้นหาวิธีการปฏิบัติเพื่อเสนอแก่บริษัทเอกชน ควรค้นหาวิธีการด้วยกระบวนการวิจัย ท่านเห็นด้วยหรือไม่ หากเห็นด้วย กระบวนการวิจัยควรใช้วิธีการวิจัยรูปแบบใด จากนั้นนำคำถามนี้ไปหาค่าความเที่ยงตรง ว่าสามารถจะตอบคำถามของวัตถุประสงค์ได้หรือไม่ โดยหาค่า IOC จากผู้เชี่ยวชาญด้านวิจัย 5 คน พบว่า ค่า IOC อยู่ที่ค่าเฉลี่ย 1.0 จึงเป็นคำถามที่สามารถจะหาคำตอบ ตอบวัตถุประสงค์ได้ ซึ่งตามเกณฑ์จะใช้ได้ ค่า IOC ตั้งแต่ 0.5 ขึ้นไป (ศิริชัย พงษ์วิชัย, 2554) เมื่อได้ข้อมูลจากการสัมภาษณ์และสนทนากลุ่มแล้ว จัดรวบรวมข้อมูลตามลำดับ เพื่อช่วยให้วิเคราะห์และตีความได้ถูกต้อง (สุภางค์ จันทวานิช, 2556)

สรุปผลการวิจัย

ขั้นตอนที่ 1 สัมภาษณ์อาจารย์ที่สอนด้านวิจัย 6 คน จากการสัมภาษณ์ได้นำคำตอบมาจัดเรียงเป็นหมวดหมู่ที่มีความเห็นสอดคล้องไปในทิศทางเดียวกัน โดยแบ่งคำตอบที่แสดงความเห็นเป็น 2 ตาราง สรุปดังนี้

ตารางที่ 1 แสดงสรุปข้อมูลที่แสดงความเห็น การค้นหาวิธีการให้พนักงานบริษัทเอกชนได้รูปแบบปฏิบัติไม่ให้ละเมิดกฎหมาย PDPA ด้วยกระบวนการวิจัย

คนที่	ความเห็น		เหตุผล
	เห็นด้วย	ไม่เห็นด้วย	
1	✓		เป็นสิ่งที่ทำให้เข้าถึงเหตุผลวิธีการดีที่สุด
2	✓		เป็นที่ยอมรับว่าอะไรยากๆ ต้องหาโดยการวิจัย
3	✓		ดีกว่ากำหนดว่าต้องทำอย่างโน้นอย่างนี้ บริษัทอาจจะไม่เชื่อ
4	✓		เป็นเรื่องใหม่ในการปฏิบัติ จึงทำวิจัยหาแนวทางถูกต้อง
5	✓		ดีกว่ากำหนดเอง มีคนมาร่วมสรุปหาวิธีการ
6	✓		เป็นการค้นหาและพิสูจน์ได้จริงไม่ใช่มาจากคนๆเดียว

จากตารางที่ 1 พบว่า ผู้ให้ข้อมูลทั้ง 6 คน แสดงความเห็นว่า ควรค้นหาวิธีการปฏิบัติตามกฎหมาย PDPA ให้ถูกต้อง ควรใช้วิธีการวิจัยด้วยเหตุผลไปในทิศทางเดียวกันว่า การวิจัยพิสูจน์ได้ หากข้อสรุปจากผู้ให้ข้อมูลไม่ใช่ถูกกำหนดโดยคน ๆ เดียว

ตารางที่ 2 แสดงสรุปข้อมูลที่แสดงความคิดเห็น การค้นหาวิธีการวิจัยว่าควรใช้วิธีการวิจัยแบบใดจึงจะเหมาะสมที่สุดในการค้นหาแนวทางปฏิบัติให้ถูกต้องตามกฎหมาย PDPA

คนที่	ความเห็นรูปแบบวิจัย	เหตุผล
1	ควรใช้รูปแบบเชิงปริมาณ รับข้อมูลด้วย SEM (สมการโครงสร้างหาปัจจัยเชิงสาเหตุ)	ได้สาเหตุ ที่สามารถจัดอันดับสำคัญมากไปสำคัญน้อยได้ดี แต่ต้องหาบริษัท ที่ร่วมมือ 10-20 เท่าของตัวแปรสังเกตุได้
คนที่	**ความเห็นรูปแบบวิจัย**	**เหตุผล**
2	ควรใช้เชิงปริมาณ จะสกัดเปรียบเทียบหรือมัลติเพิลรีเกสชั่น	ด้วยจะทราบความแตกต่างของบริบทว่า ปฏิบัติต่างกันอย่างไร หรือทราบว่าอะไรบ้าง ที่ส่งผลให้ปฏิบัติ ไม่ปฏิบัติตามกฎหมาย PDPA
3, 4, 5, 6	ความเห็นคนที่ 3,4,5,6 มีความเห็นตรงกันว่า ควรหาแนวทางและบริบทที่ร่วมมือ อาจจะไม่มาก เสนอว่าค้นหาด้วยการวิจัยแบบ R and D คือวิจัยแล้วพัฒนา แต่ควรทำ 2-3 รอบ	เป็นการค้นหาปัญหาในการปฏิบัติ และหารูปแบบในการปฏิบัติ จากนั้นนำไปปฏิบัติจริงและติดตามประเมินผล เสนอการปฏิบัติว่า พนักงานบริษัทเอกชนจะปฏิบัติได้หรือไม่ เป็นการลงมือทำจริง

จากตารางที่ 2 พบว่า รูปแบบหรือกระบวนการวิจัยที่จะหาแนวทางควรดำเนินการแบบ R and D ด้วยมีผู้เห็นด้วยมากที่สุด และเหตุผลเป็นการค้นหาคำตอบและทดลองทำจริง ก่อนประกาศเป็นแนวทางปฏิบัติ

ขั้นตอนที่ 2 นำผลจากตารางที่ 1 ไปสนทนากลุ่มกับ 6 บริษัท โดยผู้บริหารด้านทรัพยากรมนุษย์มาร่วมสนทนา

ผลจากการสนทนากลุ่ม ทั้ง 6 คน อภิปรายให้ความเห็นไปในทิศทางเดียวกันว่า ปัญหา PDPA บริษัทเอกชนมีความวิตกกังวล หากจะดำเนินการหารูปแบบแนวทางปฏิบัติให้ชัดเจนนั้น เห็นด้วย และเมื่อร่างแนวทางแล้วปฏิบัติจริงเห็นผล ทั้ง 6 คนเห็นด้วยกับรูปแบบการวิจัยแบบ R and D

สรุป/ อภิปราย

จากวัตถุประสงค์ เพื่อศึกษารูปแบบงานวิจัย ที่จะทำให้ค้นพบวิธีการปฏิบัติของบริษัทเอกชน ที่ไม่ละเมิดกฎหมาย PDPA สรุปว่า วิธีวิจัยที่จะค้นหาแนวทางการปฏิบัติของบริษัทเอกชน ไม่ละเมิดกฎหมาย PDPA เป็นการวิจัยในรูปแบบ R and D โดยที่มีข้อดี คือ เป็นแนวทางที่ค้นพบ แล้วนำไปปฏิบัติ ผู้ปฏิบัติจะมั่นใจว่า จะบรรลุผลด้วยการทดลองปฏิบัติมาแล้ว อีกทั้งการวิจัย กลุ่มเป้าหมายที่จะร่วมวิจัย ใช้จำนวนไม่มาก สอดคล้องกับหลักการวิจัย R and D ที่วาโร เพ็งสวัสดิ์ (2552) ได้เขียนรายงานในวารสารมหาวิทยาลัยราชภัฏสกลนครว่า เป็นการวิจัยที่เป็นกระบวนการวิจัยและตรวจสอบคุณภาพ เป้าหมายหลักคือ ผลลัพธ์ที่สามารถทำให้เกิดประสิทธิภาพ และสอดคล้องกับความเห็นของ ดามธรรม จินากูล (2565) ที่สรุปว่า การวิจัยรูปแบบ R and D เป็นการวิจัยที่เป็นกระบวนการใหม่ ที่พร้อมนำไปใช้เพื่อการเผยแพร่ในวงกว้างได้ดี

ข้อเสนอแนะ

1. อาจารย์มหาวิทยาลัย ควรจะเร่งดำเนินการวิจัย ในรูปแบบ R and D โดยมีเป้าหมายเพื่อกำหนดแนวทางปฏิบัติของบริษัทเอกชนที่จะปฏิบัติอย่างไร จึงจะไม่ผิดกฎหมาย PDPA โดยทำการศึกษาปัญหาวิธีการปฏิบัติที่ บริษัทเอกชนดำเนินการปฏิบัติที่ยังผิดพลาดอยู่ และหาแนวทางพิจารณาการปฏิบัติให้แก่บริษัทเอกชน โดยดำเนินการวิจัยตามรูปแบบ R and D จนได้ข้อสรุป และนำเสนอบริษัทเอกชนต่อไป

2. ผู้บริหารด้านทรัพยากรมนุษย์ของบริษัทเอกชน ควรจะดำเนินการเชิงรุก โดยพิจารณามหาวิทยาลัยที่สามรรถติดต่อได้ ชักชวนนักวิจัยในมหาวิทยาลัย ร่วมกับบริษัทเอกชน ดำเนินการวิจัยในเรื่องนี้ เป็นการเร่งด่วน

เอกสารอ้างอิง

ออพติมุส (ประเทศไทย). (2021). *ทำไมเราถึงต้องให้ความสำคัญกับ PDPA?.* เข้าถึงเมื่อ 12 กรกฎาคม 2567, สืบค้นจากhttps://optimus.co.th/important-pdpa

Amnesty International Thailand. (2020). *ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน.* เข้าถึงเมื่อ 12 กรกฎาคม 2567. สืบค้นจาก https://www.amnesty.or.th/our-work/hre/udhr/

PDPA Pro. (2020). *ทำความเข้าใจให้ดีเกี่ยวกับ PDPA ว่าสำคัญกับ HR อย่างไร*?. โพสต์เมื่อวันที่ December 30, 2020 สืบค้นจาก https://pdpa.pro/blogs/understanding-pdpa-and-hr

สถาบันวิชาการนโยบายกิจการสาธารณะกับธุรกิจและการกำกับดูแล. (2561). *หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล: สหภาพยุโรป*. เข้าถึงเมื่อ 12 กรกฎาคม 2567 สืบค้นจาก *https://www.dft.go.th/th-th/DetailHotNews/ArticleId/10986/10986GDPR*

กรมการค้าต่างประเทศ. (2024). *กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation : GDPR*. เข้าถึงเมื่อวันที่ 12 กรกฎาคม 2567. สืบค้นจาก https://www.dft.go.th/th-th/DetailHotNews/ArticleId/10986/10986GDPR

The British Standards Institution. (2024). *Privacy Information Management with ISO/IEC 27701*. สืบค้นจาก https://www.bsigroup.com/th-TH/iso-27701-privacy-information-management/

ปิยธิดา ดวดขุนทด, อดิศักดิ์ วรพิวุฒิ และ ธัญญาทิพ พิชิตการค้า. (2566). *แนวทางการคุ้มครองข้อมูลส่วนบุคคลของพนักงานบริษัทกรณีศึกษา: บริษัท เฮเฟเล่ (ประเทศไทย) จำกัด*. วารสารพัฒนาธุรกิจและอุตสาหกรรม, *3*(2), 29-42.

กมลวรรณ ตันติพิวัฒนสกุล, ชวิน อุ่นภัทร, ปรุฬห์ รุจนธำรงค์, ชลธิชา สลักศิลป์, ศุภาพิชญ์ ศิริมงคล, กนกวรรณ แย้มหงษ์, และ ชินวัจน์ แสงอังศุมาลี. (2565). *การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในการให้บริการเภสัชกรรมทางไกล: การวิจัยเชิงคุณภาพ*. วารสารกฎหมายและนโยบาย สาธารณสุข, *8*(3), 495-507.

วันพิชิต ชินตระกูลชัย. (2021). *7 สิทธิของเจ้าของข้อมูล และ 5 หน้าที่ที่องค์กรต้องทำเมื่อ PDPA บังคับใช้.* เข้าถึงเมื่อ 8 กรกฎาคม 2564. สืบค้นจาก https://openpdpa.org/7-data-subject-rights-5-things-business-have-to-done-before-pdpa-use/

Rebecca Herold, (2017). *Using ISACA Privacy Principles for GDPR Compliance*. Retrieved https://www.isaca.org/resources/news-and-trends/industry-news/2017/using-isaca-privacy-principles-for-gdpr-compliance

National institute of standards and technology. Created January 8, 2020, Updated January 22, 2024. “ PRIVACY FRAMEWORK” . https://www.nist.gov/privacy-framework/privacy-framework

ธนาคารแห่งประเทศไทย. (2565). *แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct).* กรุงเทพฯ: ธนาคารแห่งประเทศไทย.

สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย. (2565). *PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล.* ม.ป.ท.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2565). *แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.* กรุงเทพฯ: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2564). *รายงานสถานภาพการพัฒนารัฐบาลดิจิทัลของประเทศไทย ประจำปี 2564.* กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

สภาองค์กรของผู้บริโภค (2561). *ชี้ประชาชนตื่นตัว PDPA แต่ช่องโหว่กฎหมายอาจทำให้ใช้ไม่ได้จริง*, สืบค้น http://www.tcc.or.th

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562*. (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา* เล่ม 136 ตอนที่ 29 ก. หน้า 52

ศิริชัย พงษ์วิชัย. (2554). *การวิเคราะห์ข้อมูลทางสถิติด้วยคอมพิวเตอร์.* พิมพ์ครั้งที่ 22. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

สุภางค์ จันทวานิช. (2556). *การวิเคราะห์ข้อมูลในการวิจัยเชิงคุณภาพ*. พิมพ์ครั้งที่ 11. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

Morse, J.M. (1994). *Designing funded qualitative research*. In Denizin, N.K. & Lincoln, Y.S., Handbook of qualitative research (2nd ed.). Thousand Oaks, CA:Sage.

วาโร เพ็งสวัสดิ์.(2552). การวิจัยและพัฒนา. *วารสารมหาวิทยาลัยราชภัฏสกลนคร.* ปีที่ 1 ฉบับที่ 2. หน้า 1-12

ดามธรรม จินากูล.(2565). *Research and Development. หลักสูตรอบรมให้ความรู้เกี่ยวกับการวิจัยสถาบัน 2565*. มหาวิทยาลัยเทคโนโลยีสุรนารี. สืบค้น htttp://www.sut.ac.th>docume

European Data Protection Board. (2023). *Guidelines on personal data breach notification under GDPR.* Brussels: EDPB.

Information Commissioner's Office. (2022). *Guide to the General Data Protection Regulation (GDPR)*. Wilmslow: ICO.

Kuner, C. (2020). *European data protection law*. Oxford: Oxford University Press.

National Institute of Standards and Technology. (2023). *Privacy framework: A tool for improving privacy through enterprise risk management*. Gaithersburg: NIST.

Solove, D. J., & Schwartz, P. M. (2022). *Privacy law fundamentals*. Portsmouth: International Association of Privacy Professionals.

Voigt, P., & von dem Bussche, A. (2021). *The EU general data protection regulation (GDPR): A practical guide.* Cham: Springer.