ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นายอริยะ ตังสวานิช

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ ไม่สังกัดภาควิชา/เทียบเท่า
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2564

Problems concerning Performance of Data Protection Officer in Financial Institutions under Personal Data Protection Act B.E. 2562

Mr. Ariya Tangsawanit

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws in Laws
Common Course
FACULTY OF LAW
Chulalongkorn University
Academic Year 2021

หัวข้อวิทยานิพนธ์	ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
โดย	นายอริยะ ตังสวานิช
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ปิยะบุตร บุญอร่ามเรือง

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

---------- คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปารีณา ศรีวนิชย์)

คณะกรรมการสอบวิทยานิพนธ์

---------- ประธานกรรมการ
(อาจารย์เข็มจริยา ธีรพงษ์)

---------- อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ปิยะบุตร บุญอร่ามเรือง)

---------- กรรมการภายนอกมหาวิทยาลัย
(อาจารย์ ดร.พีรพัฒ โชคสุวัฒนสกุล)

อริยะ ตังสวานิช : ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (Problems concerning Performance of Data Protection Officer in Financial Institutions under Personal Data Protection Act B.E. 2562) อ.ที่ปรึกษาหลัก : ผศ. ดร.ปิยะบุตร บุญอร่ามเรือง

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์ที่จะศึกษาปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในสถาบันการเงินที่เกิดขึ้นจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 โดยศึกษาประกอบกับการสัมภาษณ์ DPO ของสถาบันการเงิน 13 แห่ง รวมถึงเจ้าหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อนำมาวิเคราะห์เปรียบเทียบและนำเสนอการกำหนดโครงสร้างองค์กรและคุณสมบัติของ DPO สถาบันการเงินที่เหมาะสมต่อไป

ผลการศึกษาพบว่า มีความไม่ชัดเจนในการกำหนดโครงสร้างการทำงานของ DPO และการกำหนดคุณสมบัติของ DPO ที่เป็นมาตรฐานของสถาบันการเงินส่งผลให้เกิดปัญหาบางประการดังนี้ DPO ขาดความเป็นอิสระในการปฏิบัติหน้าที่และเกิดความขัดแย้งทางผลประโยชน์ ไม่มีการกำหนดกระบวนการปรึกษาหารือระหว่างฝ่ายงานกับ DPO ที่ครอบคลุมทั้งกระบวนการใช้ข้อมูลส่วนบุคคล ขาดพนักงานที่มีความรู้ความเข้าใจและเครื่องมือที่ใช้ในการรักษาความปลอดภัยของข้อมูล นอกจากนี้ ยังพบว่าไม่มีการกำหนดระยะเวลาการทบทวนตำแหน่ง DPO สถานะทางกฎหมายของตำแหน่งผู้ช่วย DPO และวิธีการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลขององค์กร

ด้วยเหตุตามที่กล่าวข้างต้น ผู้เขียนจึงขอเสนอให้หน่วยงานกำกับดูแลที่เกี่ยวข้องออกมาตรการทางกฎหมายเกี่ยวกับตำแหน่งหน้าที่ DPO ในสถาบันการเงิน ตลอดจนกำหนดมาตรฐานการทบทวนการประมวลผลข้อมูลส่วนบุคคลที่ชัดเจน เพื่อให้การทำงานของ DPO ในสถาบันการเงินต่างๆ สัมฤทธิ์ผลในทางกฎหมายไปพร้อมกับเกิดประโยชน์ในการแข่งขันทางธุรกิจดิจิทัล

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2564 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6280188334 : MAJOR LAWS

KEYWORD: Personal Data Protection Act B.E. 2562, Data Protection Officer, DPO, Personal Information, Data Privacy, Financial Institution

Ariya Tangsawanit : Problems concerning Performance of Data Protection Officer in Financial Institutions under Personal Data Protection Act B.E. 2562. Advisor: Asst. Prof. PIYABUTR BUNARAMRUEANG, Ph.D.

This study aims to research on the problems of Data Protection Officer (DPO) in Financial Institution in the view of the Personal Data Protection Act B.E. 2562 (PDPA) by interviewing 13 data protection officers of Financial Institutions and the staff of Office of the Personal Data Protection Commission (PDPC) to analyze, compare, and propose the suitable organizational structure and competency of DPO in Thai Financial Institutions.

According to the result of the study, the ambiguity of financial institution standard related to the organizational structure and competency of DPO cause certain issues: lack of independence and cause conflict of interest for DPO, no comprehensive advisory process between departments and DPO, insufficient staffs and tools to maintain information security. Furthermore, there is no provision on term of appointment of DPO, assistant DPO's legal status, and how to monitor processing activities of an organization.

As previously mentioned, to ensuring the law enforcement as well as encourage digital business competition, the author of this thesis recommends that Data Protection Regulators enact the specific legal measure related to the role of DPO in Financial Institutions and detailed PDPA compliance monitoring standard.

Field of Study: Laws Student's Signature .....

Academic Year: 2021 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ไม่อาจสำเร็จได้หากไม่ได้รับความกรุณาอย่างยิ่งจากอาจารย์เข็มจริยา ธีรพงษ์ ซึ่งเป็นประธานกรรมการสอบวิทยานิพนธ์ที่ได้สละเวลาอันมีค่าให้คำปรึกษา และชี้แนะแนวทางในการศึกษา และผู้ช่วยศาสตราจารย์ดร. ปิยะบุตร บุญอร่ามเรืองที่รับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ทั้งได้สละเวลาอันมีค่าให้คำปรึกษา พร้อมชี้แนะแนวทาง และให้ความเห็นเพื่อให้วิทยานิพนธ์มีเนื้อหาครบถ้วนรอบด้าน และอาจารย์ดร. พีรพัฒ โชคสุวัฒนสกุล กรรมการสอบวิทยานิพนธ์ สำหรับคำแนะนำทางด้านวิชาการ ความเห็นและแหล่งข้อมูลที่เป็นประโยชน์ต่อการจัดทำวิทยานิพนธ์เล่มนี้จนเสร็จสมบูรณ์

ขอขอบพระคุณ ผู้ให้สัมภาษณ์ทุกท่านจากธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ดร.สุนทรีย์ ส่งเสริม คุณวีระ ประเสริฐนุกูล คุณชุติมา บุญมี และผู้ที่เกี่ยวข้องที่เสียสละเวลาอันมีค่าให้สัมภาษณ์ประกอบวิทยานิพนธ์ฉบับนี้ และขอขอบพระคุณพี่หมวย พี่เพชร และเจ้าหน้าที่ประจำหลักสูตรนิติศาสตรมหาบัณฑิตทุกท่านที่ให้ ความช่วยเหลืออย่างเต็มที่จนวิทยานิพนธ์เสร็จสมบูรณ์

ขอขอบพระคุณ คุณพ่อนิติพนธ์ ตังสวานิช และคุณแม่สุธีรา บุรภัทรณิชกุล ผู้อยู่เบื้องหลังทุกความสำเร็จในชีวิตของผู้เขียน ทั้งคอยอบรมสั่งสอน ให้กำลังใจและสนับสนุนการศึกษาอย่างไม่มีที่สิ้นสุด และขอบคุณนายคชินทร์ ตังสวานิช พี่ชายที่คอยอยู่เคียงข้างในทุกๆ เรื่องมาโดยตลอด และ ขอขอบคุณนางสาวมาศิธร บุญเสริม และนายพลัฏฐ์ พิเชฐวรกุล และนายวสุ อธิชาติกุล ที่คอยช่วยเหลือสนับสนุนให้คำปรึกษา คำแนะนำ ให้กำลังใจผู้เขียน หากไม่มีบุคคลเหล่านี้วิทยานิพนธ์เล่มนี้ไม่อาจเสร็จสมบูรณ์ได้

ขอขอบคุณนางสาวทศพร นางสาวมนธิดา นายจักรกฤษณ์ นายพีรวัส นายพีระติ นางสาวสวิตรี นางสาวพิชญ์สินี นางสาวมฤษฎา นางสาวชนนิกานต์ นาวสาวธมลวรรณ นางสาวนัศรา นายณัฐวีร์ นายพบธรรม นายธีร์ นางสาวการเกตุ นายพงศธร และเพื่อนๆ ปริญญาโท ปริญญาตรี และมัธยมที่ไม่ได้กล่าวถึง ณ ที่นี้ แต่ให้ความช่วยเหลือและเป็นกำลังใจตั้งแต่เข้าศึกษาจน ผู้เขียนสำเร็จการศึกษา

ท้ายนี้ ผู้เขียนหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์เล่มนี้จะก่อให้เกิดประโยชน์แก่ผู้ที่สนใจจะศึกษาและเป็นแนวทางในการศึกษาเรื่องนี้ต่อไปในอนาคต หากมีข้อผิดพลาดประการใด ผู้เขียนขอน้อมรับไว้เพียงผู้เดียวและขออภัยไว้ ณ ที่นี้

อริยะ ตังสวานิช

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

สารบัญอักษรย่อและคำศัพท์ที่ใช้

GDPR หรือ The EU General Data Protection Regulation	กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้ในสหภาพยุโรป
European Data Protection Supervisor หรือ EDPS	หน่วยงานคุ้มครองข้อมูลที่รับผิดชอบตรวจสอบว่าองค์กรในยุโรปปฏิบัติตามกฎหมายคุ้มครองข้อมูลของยุโรป
ICO หรือ UK Information Commissioner's Office	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร
The Article 29 Working Party หรือ WP29	คณะทำงานตามมาตรา 29 ก่อนที่จะกลายเป็นคณะกรรมการคุ้มครองข้อมูลแห่งยุโรป (EDPB)
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
Data Protection Officer หรือ DPO	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
Three Lines of Defense	หลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ
สถาบันการเงิน	สถาบันการเงินในที่นี้ หมายถึง ธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจ
ธปท.	ธนาคารแห่งประเทศไทย
สคส.	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
DPIA	การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
Legitimate Interest Assessment หรือ LIA	การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
ROPA	บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
Personal Data Breach	เหตุละเมิดข้อมูลส่วนบุคคล ซึ่งทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง เปิดเผยหรือเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
Privacy Notice	ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล
Data Processing Agreement หรือ DPA	ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
Data Subject Request หรือ DSR	คำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของปัญหา

กระแสการคุ้มครองข้อมูลส่วนบุคคลในยุคเศรษฐกิจดิจิทัลปัจจุบันนั้นเกิดการเปลี่ยนแปลงอย่างรวดเร็ว มีคำกล่าวว่า “Data is the new oil.” หรือข้อมูลเริ่มมีความสำคัญมากขึ้นจนกลายเป็นแหล่งสร้างกำไรและมูลค่าของแต่ละองค์กร ดังนั้น ข้อมูลส่วนบุคคลจึงไม่ใช่เรื่องของการเก็บรักษาเป็นความลับที่จะสามารถใช้หรือเปิดเผยได้เมื่อได้รับความยินยอมอย่างชัดเจนของเจ้าของข้อมูลเพียงอย่างเดียวอีกต่อไป ในปัจจุบันการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล หรือที่เรียกกันว่าการประมวลผลข้อมูล (Data Processing) เป็นสิ่งที่ยอมรับกันว่าสามารถกระทำได้แต่จะต้องเป็นการประมวลผลข้อมูลอย่างปลอดภัยและได้มาตรฐานสากล

ยิ่งความสำคัญของข้อมูลมีเพิ่มมากขึ้นเท่าไรอาชญากรรมทางข้อมูลและความเป็นไปได้ที่ข้อมูลจะรั่วไหลก็เพิ่มขึ้นตามมา เช่น การตัดต่อใบหน้าเพื่อหลอกลวงผู้อื่นด้วยการสร้างวิดีโอปลอม (Deepfake) การสร้างข่าวจริงด้านลบของบุคคลหรือองค์กรใดขึ้นลงในสื่อโซเชียลอย่างต่อเนื่องเพื่อตอกย้ำภาพด้านลบจนกลายเป็นความเชื่อถาวร (Brainwashing) หรือการที่เจ้าของแพลตฟอร์มให้บริการเก็บข้อมูลส่วนบุคคลอาจนำข้อมูลส่วนตัวหรือข้อมูลธุรกิจของผู้ใช้บริการไปวิเคราะห์ข้อมูลเชิงลึกเพื่อศึกษาพฤติกรรมของผู้ใช้แต่ละรายเพื่อนาเสนอสินค้าและบริการที่เข้าถึงผู้ใช้ได้โดยตรงซึ่งนับว่าเป็นการรุกล้ำความเป็นส่วนตัว[1] เป็นต้น จะเห็นได้ว่าการคุ้มครองข้อมูลส่วนบุคคลจึงไม่ใช่เรื่องของการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพียงอย่างเดียวเท่านั้น แต่หมายถึงการบริหารจัดการความเสี่ยงด้านข้อมูลและความเสี่ยงต่อความเป็นส่วนตัวที่จะอาจเกิดขึ้นได้จากการประกอบธุรกิจ และการคุ้มครองความเชื่อมั่นของเจ้าของข้อมูลส่วนบุคคล ตลอดจนการรักษาภาพลักษณ์ที่ดีขององค์กรซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

[1] ดร.ปริญญา หอมเอนก, "10 แนวโน้ม Cybersecurity and Privacy Trends 2020" [ออนไลน์] เข้าถึงเมื่อ 21 ตุลาคม 2563. แหล่งที่มา: https://www.bangkokbiznews.com/blog/detail/649796

ธนาคารแห่งประเทศไทยเล็งเห็นว่าข้อมูลเป็นพื้นฐานสำคัญในการตัดสินใจเชิงนโยบายหลายด้าน กลไกสำคัญที่จะช่วยเสริมสร้างให้สถาบันการเงินบริหารจัดการข้อมูลเป็นไปตามวัตถุประสงค์ของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล คือ การมีส่วนร่วมและการประสานงานในทุกระดับของสมาชิกในองค์กร

โดยบุคคลที่จะเข้ามาทำหน้าที่ในการตรวจสอบและให้คำแนะนำแก่สถาบันการเงินเพื่อให้การประมวลผลข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)[2] บุคคลดังกล่าวยังทำหน้าที่เป็นผู้ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล

การแต่งตั้ง DPO ของสถาบันการเงินก่อให้เกิดประโยชน์ต่อผู้มีส่วนเกี่ยวข้องกับข้อมูล (Data Stakeholder) สองประการ ประการแรก คือ ก่อให้เกิดประโยชน์กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล เนื่องจาก DPO ซึ่งเป็นผู้เชี่ยวชาญที่สถาบันการเงินตั้งขึ้นจะคอยตรวจสอบกิจกรรมการประมวลผล พร้อมทั้งให้คำแนะนำแก้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในการดำเนินการให้เป็นไปตามกฎหมาย หลักเกณฑ์ และแนวปฏิบัติที่เกี่ยวข้อง ประการที่สอง คือ DPO จะเข้ามามีส่วนช่วยรักษาความสัมพันธ์อันดีระหว่างสถาบันการเงินกับหน่วยงานกำกับดูแล และกับเจ้าของข้อมูลส่วนบุคคล โดยเป็นบุคคลที่ทำหน้าที่ติดต่อประสานงานกับบุคคลดังกล่าว หากสถาบันการเงินสามารถทำให้ DPO เข้ามามีส่วนร่วมกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามเงื่อนไขของกฎหมายและมาตรฐานสากลได้ ย่อมเป็นการสร้างความเชื่อถือรวมถึงความได้เปรียบทางธุรกิจของสถาบันการเงินแต่ละแห่ง

General Data Protection Regulation (GDPR) และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดเงื่อนไขหน้าที่และความสัมพันธ์ระหว่าง DPO กับสถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลหลายประการ เช่น DPO ต้องสามารถปฏิบัติหน้าที่ได้ด้วยวิธีการที่เป็นอิสระและสามารถรายงานให้ผู้บริหารสูงสุดของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลทราบโดยตรง รวมถึงหน้าที่หรือภารกิจของ DPO ต้องไม่ขัดกับหน้าที่ที่บุคคลนั้นมีต่อสถาบันการเงิน อย่างไรก็ดี

[2] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42

เนื่องจากความไม่ชัดเจนของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในไทยปัจจุบันก่อให้เกิดปัญหาเชิงโครงสร้างองค์กรที่มีการแต่งตั้ง DPO และปัญหาเชิงความรู้ความสามารถของ DPO ตลอดจนปัญหาทางปฏิบัติแก่การปฏิบัติงานของ DPO หลายประการ ปัญหาดังกล่าวได้แก่

1. ปัญหาเกี่ยวกับการมีส่วนเกี่ยวข้องภายในสถาบันการเงินของ DPO
2. ปัญหาด้านทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ DPO
3. ปัญหาความเป็นอิสระในการตัดสินใจ
4. ปัญหาความขัดแย้งทางผลประโยชน์ (Conflict of interest)
5. ปัญหาเรื่องระยะเวลาการดำรงตำแหน่งและการพ้นจากตำแหน่ง DPO
6. ปัญหาเกี่ยวกับสถานะทางกฎหมายของผู้ช่วย DPO และผู้แทน DPO
7. ปัญหาทางปฏิบัติของ DPO ในสถาบันการเงิน

หากปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงิน และปัญหาเชิงความสามารถของ DPO ตลอดจนปัญหาทางปฏิบัติที่ DPO และผู้ปฏิบัติงานในสถาบันการเงินต้องเผชิญนั้นไม่ได้รับการแก้ไขย่อมส่งผลกระทบต่อตำแหน่งหน้าที่และภาระงานของ DPO เนื่องจาก DPO อาจให้คำแนะนำซึ่งเป็นไปตามกฎหมายแต่ไม่สอดคล้องกับนโยบายและเป้าหมายทางธุรกิจของสถาบันการเงิน หรือปฏิบัติหน้าที่ได้อย่างไม่เหมาะสมเนื่องจาก DPO ขาดความเป็นอิสระหรือมีส่วนได้เสียขัดกันผลประโยชน์ขององค์กร หรือทำให้ DPO การตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลบกพร่อง เพราะขาดความเข้าใจกระบวนการเกี่ยวกับข้อมูลส่วนบุคคลขององค์กรอย่างแท้จริง เป็นต้น ท้ายที่สุดย่อมส่งผลกระทบต่อการคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคลอันเป็นเจตนารมณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยวิทยานิพนธ์ฉบับนี้จะชี้ให้เห็นถึงปัญหาที่เกิดขึ้นบทบัญญัติแห่งกฎหมายโดยแท้ ทั้งปัญหาเกี่ยวกับความไม่ชัดเจนของกฎหมาย รวมถึงปัญหาทางปฏิบัติที่เกิดขึ้นจริงกับการทำงานของ DPO และคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน ทั้งนี้เพื่อทำความเข้าใจลักษณะที่มา และสาเหตุของปัญหาต่างๆ พร้อมทั้งเสนอแนะแนวทางกำหนดโครงสร้างการปฏิบัติงานขององค์กรที่เหมาะสมกับ DPO การคัดเลือกบุคคลที่จะดำรงตำแหน่ง DPO ของสถาบันการเงิน ตลอดจนแนวทางแก้ไขปัญหาทางปฏิบัติที่เกิดขึ้นจากการดำเนินการตามกฎหมายของสถาบันการเงินในประเทศไทยแต่ละแห่ง

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาบทบาทหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน
2. เพื่อศึกษาปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงินที่มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน และปัญหาทางปฏิบัติอื่นๆ ที่เกิดขึ้นจากพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. เพื่อวิเคราะห์ปัญหาที่เกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน
4. เพื่อหาแนวทางการแก้ไขปัญหาและข้อเสนอแนะสำหรับการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินที่เหมาะสม

1.3 สมมติฐาน

ปัจจุบันยังไม่มีการกำหนดโครงสร้างการทำงานและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินที่ชัดเจน จึงทำให้มีปัญหาการขัดกันของการปฏิบัติหน้าที่ระหว่างบทบาทหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบทบาทหน้าของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่มีต่อองค์กร รวมถึงปัญหาด้านความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

1.4 ขอบเขตของการวิจัย

การวิจัยนี้จะมุ่งศึกษาปัญหาทางกฎหมายและปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในธุรกิจสถาบันการเงินที่เกิดขึ้นจากบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ General Data Protection Regulation (GDPR) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับในสหภาพยุโรป เพื่อหาแนวทางการแก้ไขปัญหาเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินไทย

1.5 วิธีดำเนินงานวิจัย

การศึกษาวิจัยนี้ใช้วิธีการวิจัยเอกสารด้วยการค้นคว้าและรวบรวมข้อมูลทางเอกสารที่เกี่ยวข้อง (Documentary Research) โดยจะทำการศึกษาและวิเคราะห์ข้อมูลจากเอกสาร เช่น กฎหมายภายในของประเทศไทย กฎหมายต่างประเทศ มาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เอกสารทางวิชาการ วิทยานิพนธ์ วารสารกฎหมาย ฐานข้อมูลทางอินเตอร์เน็ต รวมถึงการวิจัยภาคสนาม (Qualitative Research) โดยสัมภาษณ์เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้ที่เกี่ยวข้องในสถาบันการเงินไทยแต่ละแห่ง

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบและเข้าใจลักษณะหน้าที่ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินตามกฎหมายและตามสภาพการปฏิบัติงานจริง
2. ทำให้ทราบและเข้าใจปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงินที่มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และปัญหาทางปฏิบัติอื่นๆ ที่เกิดขึ้นจากพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ
3. ทำให้ทราบถึงผลการวิเคราะห์ปัญหาที่เกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน
4. ทำให้เกิดแนวทางการแก้ไขปัญหาและข้อเสนอแนะในการจัดโครงสร้างสถาบันการเงินที่สอดคล้องกับการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตลอดจนคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

บทที่ 2

ภาพรวมเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน

การประกอบกิจการของสถาบันการเงินของประเทศไทยนั้นอยู่ภายใต้การกำกับดูแลอย่างเข้มงวด ดังจะเห็นได้จากการที่ธนาคารแห่งประเทศไทยออกประกาศหลักเกณฑ์เกี่ยวกับการกำกับดูแลการดำเนินธุรกิจและการรักษาความปลอดภัยของข้อมูลลูกค้าอย่างมากมาย เช่น ประกาศของธนาคารแห่งประเทศไทยเรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ประกาศธนาคารแห่งประเทศไทยเรื่องหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการสนับสนุนการประกอบธุรกิจ (Business facilitator) หรือประกาศธนาคารแห่งประเทศไทยเรื่องหลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอกในการประกอบธุรกิจของสถาบันการเงิน (Outsourcing) ล่าสุดได้ออกแนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance) เพื่อให้ข้อมูลทั้งหมดของสถาบันการเงินมีการกำกับดูแลที่ครอบคลุมทั้งองค์กรต่อเนื่อง รวมทั้งเพื่อให้ข้อมูลขององค์กรมีคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และเป็นประโยชน์ต่อการดำเนินธุรกิจ บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

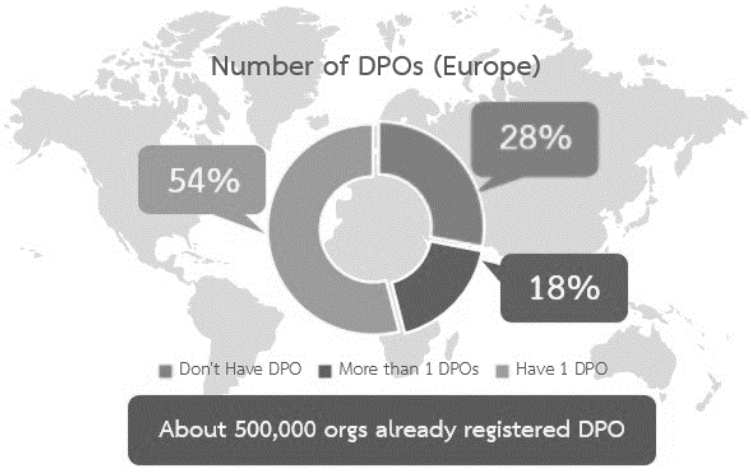
แต่เดิมก่อนที่จะมีการให้ความสำคัญในการให้ความคุ้มครองข้อมูลส่วนบุคคลนั้น สถาบันการเงินจะมีนโยบายในการเก็บรักษาข้อมูลลูกค้าไว้เป็นความลับ และประพฤติปฏิบัติต่อกันเรื่อยมาจนกลายเป็นจารีตประเพณี[1] อย่างไรก็ดี แนวคิดในการปฏิบัติต่อข้อมูลส่วนบุคคลของลูกค้าสถาบันการเงินได้มีการเปลี่ยนแปลงไปจากเดิมซึ่งเน้นการขอความยินยอมจากลูกค้า (consent) กลายเป็นแนวคิดว่าข้อมูลส่วนบุคคลเป็นทรัพยากรที่สถาบันการเงินต้องนำไปใช้เพื่อให้เกิดประโยชน์ในการประกอบกิจการแต่ต้องเป็นการใช้อย่างปลอดภัยและได้มาตรฐานสากล เพื่อทำให้ลูกค้าเกิดความเชื่อมั่นว่าสถาบันการเงินจะนำข้อมูลส่วนบุคคลของตนไปใช้อย่างปลอดภัย โปร่งใสและเป็นธรรม รวมถึงเป็นประโยชน์ต่อภาพลักษณ์ในการทำธุรกิจขององค์กรทั้งภายในประเทศและกับต่างประเทศ กล่าวคือ สถาบันการเงินสามารถประมวลผลข้อมูลส่วนบุคคลที่ได้หากมีฐานหรือเหตุผลในการ

[1] กุลโมไนย พิทักษ์โชติไชย, มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสถาบันการเงิน (หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยเกริก: 2556), หน้า.2

ประมวลผลตามกฎหมาย (lawful basis)[2] เช่น ฐานประโยชน์โดยชอบธรรม (legitimate interest) มิได้จำกัดว่าสถาบันการเงินจะต้องเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าไว้เป็นความลับ และจะต้องขอความยินยอมเมื่อต้องการใช้ข้อมูลของลูกค้าในทุกกรณีอีกต่อไป

ในยุคเศรษฐกิจดิจิทัลปัจจุบัน บุคคลที่มีความสำคัญอย่างมากบุคคลหนึ่งที่ทำหน้าที่ในการให้คำปรึกษาและตรวจสอบดูแลให้กระบวนการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรฐานสากลที่เกี่ยวข้อง คือ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)” เมื่อปี ค.ศ. 2019 ภายหลังจากที่ GDPR มีผลใช้บังคับไปแล้วสองปีมีการประเมินว่าองค์กรในสหภาพยุโรปกว่า 500,000 องค์กรได้มีการแต่งตั้ง DPO เป็นของตนเองแล้ว และจากผลสำรวจ 370 องค์กรนั้นปรากฏว่าได้แต่งตั้ง DPO จากบุคคลภายในองค์กรประมาณ 72% จากการแต่งตั้งทั้งหมด โดยแบ่งเป็นการตั้งบุคคลคนเดียวเป็น DPO จำนวน 54% และการตั้งทีมงาน DPO เป็นจำนวน 18%[3]

ภาพที่ 1 จำนวน DPO ขององค์กรในสหภาพยุโรป



ที่มา: IAPP-EY Annual Privacy Governance Report 2019

[2] ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, Thailand Data Protection Guideline 2.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย: ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2562), หน้า.83.

[3] IAPP-EY, "IAPP-EY Annual Privacy Governance Report 2019," [Online] Accessed: 16 Nov 2020. Available from: https://iapp.org/store/books/a191P000003Qv5xQAC/

ในการกำกับดูแลการดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สถาบันการเงินซึ่งจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยมีเหตุที่มีข้อมูลส่วนบุคคลของลูกค้าจำนวนมาก (large scale)[4] กล่าวคือ ประมวลผลข้อมูลส่วนบุคคลของลูกค้าตามกิจธุระปกติหรือมีข้อมูลส่วนบุคคลของเจ้าของข้อมูลอยู่ภายในรอบระยะเวลาสิบสองเดือนมากกว่า 50,000 รายหรือมากกว่า 5,000 รายในกรณีเป็นข้อมูลอ่อนไหว[5] กฎหมายกำหนดให้ต้องมีแต่งตั้ง DPO[6] โดยหน้าที่และความรับผิดชอบของ DPO อาจแบ่งออกได้เป็น 4 ประการ[7] ดังต่อไปนี้

ภาพที่ 2 บทบาทหน้าที่ของ DPO

(1) ให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Advisory)[8]

DPO มีหน้าที่ให้คำแนะนำในการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย รวมถึงให้คำแนะนำในการประเมินผลกระทบด้านการ

[4] WP29: Guidelines on Data Protection Officers (‘DPOs’) (การประมวลผลข้อมูลจำนวนมากควรคำนึงถึงปัจจัยหลายอย่าง ได้แก่ จำนวนเจ้าของข้อมูลส่วนบุคคล ปริมาณข้อมูลหรือลักษณะของข้อมูลที่ทำการประมวลผล ระยะเวลาของกิจกรรมการประมวลผล และขอบเขตทางด้านภูมิศาสตร์ของกิจกรรมการประมวลผล โดยการประมวลผลข้อมูลส่วนบุคคลของลูกค้าในธุรกิจบริษัทประกันและธนาคารถือว่าเป็นการประมวลผลข้อมูลจำนวนมากธุรกิจหนึ่ง)

[5] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.5. โปรดดู https://www.law.chula.ac.th/event/10941/

[6] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41(2)

[7] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 และ General Data Protection Regulation (GDPR), Article 39(1)

[8] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(1)

คุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA)[9] บุคคลที่จะทำเข้ารับตำแหน่ง DPO ของสถาบันการเงินจึงจำเป็นต้องเข้าใจวัฒนธรรมการดำเนินงาน วัตถุประสงค์ขององค์กร กระบวนการปฏิบัติงาน กิจกรรมการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินนั้นๆ และการไหลเวียนของข้อมูลส่วนบุคคล (data flow) ภายในสถาบันการเงิน โดยต้องติดตามการเปลี่ยนแปลงของมาตรการ กฎระเบียบต่างๆ รวมถึงแนวทางคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศอยู่ตลอดเวลา รวมถึงสร้างความตระหนักรู้ภายในสถาบันการเงินและฝึกอบรมพนักงานที่มีส่วนเกี่ยวข้องในการกระบวนการประมวลผลข้อมูลส่วนบุคคล[10] เพื่อที่จะให้คำแนะนำที่เป็นประโยชน์กับสถาบันการเงินทั้งในแง่การประกอบธุรกิจและแง่ของการปฏิบัติตามกฎหมาย

(2) ตรวจสอบการประมวลผลข้อมูลส่วนบุคคลขององค์กร (Monitoring)[11]

DPO จะต้องติดตามและตรวจสอบอย่างสม่ำเสมอว่าสถาบันการเงินมีนโยบายการคุ้มครองข้อมูลส่วนบุคคลและข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามกฎ ระเบียบข้อบังคับภายในองค์กร และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล[12] รวมถึงหน้าที่ใน

---

[9] Article 29 Data Protection Working Party (WP29), "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," [Online] Accessed: 20 Jan 2021. Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 (ในกรณีที่ชุดข้อมูลมีความเสี่ยงสูง ผู้ประมวลผลข้อมูลจะต้องจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูล ส่วนบุคคล (DPIA) โดยขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การประเมินนั้นจะต้องกระทำก่อนหรือในขณะที่มีการประมวลผลข้อมูลส่วนบุคคล รวมถึงการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่แล้ว โดยพิจารณาจากลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลร่วมด้วย)

[10] Douwe Korff and Marie Georges, "The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation," [Online] Accessed: 22 Jan 2021. Available from: https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf. pp.243-244.

[11] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(2)

[12] สำหรับหน้าที่ในการตรวจสอบการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ WP29: Guidelines on Data Protection Officers (‘DPOs’) ได้คำแนะนำว่า DPO ควรทำกิจกรรมดังต่อไปนี้อย่างต่อเนื่อง

- เก็บรวบรวมข้อมูลเพื่อระบุกิจกรรมการประมวลผล
- วิเคราะห์และตรวจสอบการปฏิบัติตามในแต่ละกิจกรรมการประมวลผล
- แจ้งให้ทราบ ให้คำปรึกษา และให้คำแนะนำในประเด็นที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลพบเจอ

การรับมือกับเหตุละเมิดข้อมูลส่วนบุคคล[13] การสอบสวนสิ่งผิดปกติตามคำร้องเรียนของบุคคลต่างๆ รวมถึงการที่หน่วยธุรกิจไม่ปฏิบัติตามคำแนะนำโดยไม่มีเหตุผลอันสมควร และรายงานเรื่องดังกล่าวให้ผู้บริหารระดับสูงและเจ้าของข้อมูลทราบ[14]

(3) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Cooperation with the Data Protection Authority)[15]

DPO เป็นผู้ประสานงานหลักและทำหน้าที่ตอบรับคำร้องของหน่วยงานกำกับดูแล เมื่อ สคส. หรือหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง ต้องการเอกสารหรือข้อมูลใดเพื่อใช้ในการสอบสวน แก้ไข หรืออนุมัติ ตลอดจน DPO สามารถขอคำปรึกษากับหน่วยงานกำกับดูแลเพื่อประโยชน์ในการดูแลตรวจสอบให้การดำเนินการของสถาบันการเงินเป็นไปตามกฎหมาย[16] ในขณะเดียวกัน หน่วยงานกำกับดูแลควรให้ความช่วยเหลือในด้านต่างๆ แก่การปฏิบัติหน้าที่ของ DPO รวมถึงความช่วยเหลือในด้านการตีความกฎหมาย เพื่อให้เกิดมาตรการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินต่างๆ เป็นมาตรฐานเดียวกันกับหน่วยงานกำกับดูแล[17]

(4) หน้าที่ในการรักษาความลับ (Confidentiality Obligation)[18]

---

[13] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

[14] GDPR, Article 83 และ WP29: Guidelines on Data Protection Officers (‘DPOs’), หน้า.14. (หาก DPO พบว่าบุคคลใดไม่ให้ความร่วมมือในการสอบสวน DPO ต้องรายงานต่อผู้บริหารสูงสุดของสถาบันการเงิน ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 42 วรรคสาม ซึ่งผู้บริหารระดับสูงมีหน้าที่แก้ไขปรับปรุง รวมไปถึงการลงโทษบุคคลของสถาบันการเงินที่ปฏิบัติหน้าที่บกพร่อง เช่น ออกจดหมายเตือน ใช้มาตรการลงโทษต่างๆ หรืออาจให้ออกจากงานหรือยกเลิกสัญญาในกรณีร้ายแรง เป็นต้น และหากสถาบันการเงินละเลยการตรวจสอบอาจถูกหน่วยงานกำกับดูแลลงโทษได้)

[15] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(3)

[16] EDPS, "Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001," [Online] Accessed: 7 Jan 2021. Available from: https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf, pp.10-11. (DPO จึงควรถูกมองว่าเป็นเจ้าหน้าที่ของสถาบันการเงิน มิใช่ตัวแทนของ สคส. เพราะ DPO มีหน้าที่ตรวจสอบจากภายในองค์กรว่าสถาบันการเงินทำตามกฎหมาย ให้คำแนะนำและจัดการแก้ไขเมื่อพบการไม่ปฏิบัติตาม เพื่อไม่ให้เกิดกรณีที่ สคส. เข้ามาแทรกแซงการปฏิบัติงานขององค์กร)

[17] GDPR, Article 57(1)(c)

[18] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(4)

DPO มีหน้าที่รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมาย หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลฝ่าฝืนโดยนำไปเปิดเผยแก่ผู้อื่นต้องระวางโทษตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย เช่น[19] การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ เป็นต้น

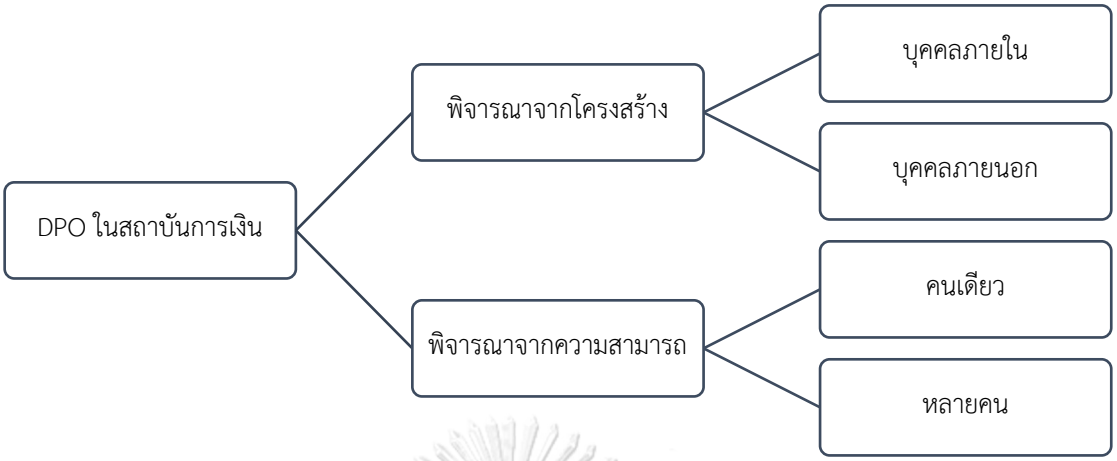
ในส่วนถัดไป ผู้เขียนจะกล่าวถึงที่มาของ DPO ในสถาบันการเงิน กล่าวคือ สถาบันการเงินเลือกแต่งตั้งผู้ปฏิบัติหน้าที่ในฐานะ DPO เป็นบุคคลคนเดียวหรือเป็นบุคคลหลายคน สถาบันการเงินแต่งตั้งบุคคลดังกล่าวจากพนักงานภายในองค์กรหรือว่าจ้างให้บุคคลภายนอกทำหน้าที่รับผิดชอบ

2.1 ที่มาของ DPO ในสถาบันการเงิน

สำหรับการศึกษาว่าการแต่งตั้ง DPO ในประเทศไทยเป็นอย่างไร โดยเบื้องต้นผู้เขียนคาดการณ์รูปแบบที่มาของการแต่งตั้ง DPO ซึ่งแบ่งออกได้เป็น 2 กลุ่ม ได้แก่ (1) การแต่งตั้ง DPO โดยพิจารณาจากโครงสร้างองค์กรของสถาบันการเงินในประเทศไทย และ (2) การแต่งตั้ง DPO โดยพิจารณาจากความรู้ความสามารถส่วนตัวของบุคคลที่จะเข้ามารับตำแหน่ง DPO ของสถาบันการเงิน

[19] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guildlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension) (โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย: 2564), หน้า.582.

ภาพที่ 3 ที่มาของ DPO ในสถาบันการเงิน



2.1.1 แต่งตั้งโดยพิจารณาจากโครงสร้างองค์กรสถาบันการเงิน

สถาบันการเงินสามารถแต่งตั้ง DPO ได้โดยพิจารณาจากโครงสร้างองค์กรว่ามีความเหมาะสมต่อการปฏิบัติหน้าที่ของ DPO ตามกฎหมายหรือไม่ หากสถาบันการเงินเลือกที่จะ DPO จากบุคคลภายในองค์กรจะต้องมีการปรับโครงสร้างองค์กรให้สอดคล้องกับสถานะทางกฎหมายของ DPO[20] หรืออาจเลือกทำสัญญาให้บุคคลภายนอกทำหน้าที่เป็น DPO หรืออาจใช้ DPO ร่วมกันกับสถาบันการเงินอื่นก็ได้[21]

1) บุคคลภายในสถาบันการเงิน (In-house)

หากสถาบันการเงินมีบุคลากรภายในองค์กรที่มีความรู้ความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลและความเข้าใจในกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเป็นอย่างดีอยู่แล้ว สถาบันการเงินอาจแต่งตั้งให้บุคคลดังกล่าวเป็น DPO เนื่องจากตามกฎหมายนั้น DPO อาจเป็นลูกจ้างหรือพนักงานของสถาบันการเงินพร้อมกับการปฏิบัติหน้าที่อื่นในองค์กรได้ตราบเท่าที่สถาบันการเงินรับรองได้ว่าการปฏิบัติหน้าที่ของบุคคลดังกล่าวไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ในฐานะ DPO[22] หรือเรียกว่าไม่มีความขัดแย้งทางผลประโยชน์ (Conflict of Interest) ซึ่งผู้เขียนจะกล่าวถึงปัญหาเกี่ยวกับความขัดแย้งทางผลประโยชน์ต่อไปใน “หัวข้อ 3.4 ความขัดแย้งทางผลประโยชน์”

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสอง ถึง วรรคสี่

[21] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41 วรรคสอง

[22] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคท้าย

อนึ่ง มีข้อพิจารณาประการหนึ่งในกรณีที่สถาบันการเงินแต่งตั้งบุคคลภายในองค์กรเป็น DPO เพื่อปฏิบัติหน้าที่ตามกฎหมาย คือ หากบุคคลนั้นเป็นกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ หรือที่ปรึกษาของสถาบันการเงิน[23] กฎหมายจะกำหนดให้สถาบันการเงินมีหน้าที่ดำเนินการตามกระบวนการขั้นตอนหลายประการ กล่าวคือ สถาบันการเงินต้องยื่นขอหารือ ขอความเห็นชอบ รวมถึงแจ้งการแต่งตั้งหรือการเปลี่ยนแปลงบุคคลนั้นซึ่งเป็นกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ ที่ปรึกษาของสถาบันการเงิน หรือผู้บริหารในตำแหน่งสูงสุดอื่นๆ มายังธนาคารแห่งประเทศไทย[24] ซึ่งสามารถสรุปได้ดังตารางด้านล่างนี้

[23] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 10/2561 ธรรมาภิบาลของสถาบันการเงิน และ ประกาศธนาคารแห่งประเทศไทยที่ สกส. 12/2562 ธรรมาภิบาลของสถาบันการเงินเฉพาะกิจ “ที่ปรึกษาของสถาบันการเงิน หมายความว่า บุคคลที่เป็นที่ปรึกษาของสถาบันการเงิน หรือบุคคลที่อาจทำหน้าที่เปรียบเสมือนกรรมการ ผู้จัดการ รองผู้จัดการ หรือผู้ช่วยผู้จัดการ แต่เพียงใช้ชื่อว่าเป็นที่ปรึกษาเท่านั้น รวมไปถึงบุคคลที่มีลักษณะดังกล่าว แต่เรียกชื่ออย่างอื่นด้วย อย่างไรก็ตาม ไม่รวมถึงบุคคลที่รับจ้างทำงานให้แก่สถาบันการเงิน โดยมีลักษณะของงานที่ใช้ความรู้ความสามารถพิเศษด้านเทคนิค หรือใช้ความชานาญเฉพาะด้าน เช่น ที่ปรึกษางานบัญชี ที่ปรึกษากฎหมาย ที่ปรึกษาเทคโนโลยีสารสนเทศ ที่ปรึกษาด้านภาษี ที่ปรึกษาด้านภาษา ที่ปรึกษาด้านการสื่อสารองค์กร ที่ปรึกษาด้านประกันภัย ที่ปรึกษาด้านแบบจำลองเชิงปริมาณขั้นสูง เป็นต้น”

[24] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 3/2564 เรื่อง หลักเกณฑ์การพิจารณาให้ความเห็นชอบการแต่งตั้งกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ หรือที่ปรึกษาของสถาบันการเงิน บริษัทแม่ของสถาบันการเงิน และบริษัทลูกที่ประกอบธุรกิจทางการเงิน

ตารางที่ 1 การยื่นคำขอหารือ ความเห็นชอบ การแจ้งการแต่งตั้งหรือการเปลี่ยนแปลงกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ ที่ปรึกษาของสถาบันการเงิน

	1. การขอหารือ	2. การขอความเห็นชอบ[25]	3. การแจ้งการแต่งตั้ง/ การเปลี่ยนแปลง[26]
กรรมการ	✓รายใหม่*	✓	✓
ผู้มีอำนาจในการจัดการ			
- ผู้จัดการ	✓รายใหม่*	✓**	✓
- รองผู้จัดการ/ผู้ช่วยผู้จัดการ		✓	✓
ที่ปรึกษาของสถาบันการเงิน		✓	✓

หมายเหตุ: * รายใหม่ หมายถึง กรรมการ ผู้จัดการ หรือตำแหน่งเทียบเท่าที่เรียกชื่ออย่างอื่น ซึ่งเป็นบุคคลที่ยังไม่เคยได้รับความเห็นชอบจากธนาคารแห่งประเทศไทยในการดำรงตำแหน่งใดๆ ในสถาบันการเงินมาก่อน

** ผู้บริหารในตำแหน่งสูงสุดของสถาบันการเงิน ต้องขอความเห็นชอบทุกครั้งก่อนที่ จะมีการต่อวาระหรืออายุสัญญาเพื่อให้ดำรงตำแหน่งต่อไป หรือทุก 4 ปี นับแต่วันที่บุคคลดังกล่าวได้รับการแต่งตั้งให้ดำรงตำแหน่ง แล้วแต่เวลาใดจะถึงก่อน

ที่มา: คู่มือสำหรับประชาชน : การขอความเห็นชอบการแต่งตั้งหรือแจ้งเปลี่ยนแปลงกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ หรือที่ปรึกษาของสถาบันการเงิน บริษัทแม่ของสถาบันการเงิน และผู้บริหารในตำแหน่งสูงสุดของบริษัทลูกในกลุ่ม Solo Consolidation

นอกจากกระบวนการกำกับดูแลกิจการสถาบันการเงินข้างต้น ในกรณีการแต่งตั้งบุคคลภายในสถาบันการเงินเป็น DPO จะต้องคำนึงถึงโครงสร้างองค์กรและสายบังคับบัญชาของ DPO โดยธนาคารแห่งประเทศไทยกำหนดให้สถาบันการเงินมีโครงสร้างองค์กรที่เอื้อให้การทำหน้าที่ควบคุม กำกับ และตรวจสอบ มีความเป็นอิสระและมีประสิทธิผลเพื่อติดตามการดำเนินงานให้เป็นไปตามนโยบายและกระบวนการที่กำหนด รวมทั้งถูกต้องตามกฎหมาย กฎระเบียบข้อบังคับต่างๆ ของ

[25] ให้สถาบันการเงินมีหนังสือขอความเห็นชอบพร้อมเอกสารประกอบ ทั้งนี้ หาก ธปท. ไม่มีหนังสือแจ้งทักท้วง หรือขอข้อมูลเพิ่มเติมภายใน 15 วันทำการ นับแต่วันที่ ธปท. ได้รับหนังสือขอความเห็นชอบและเอกสารที่เกี่ยวข้องครบถ้วน ให้ถือว่า ธปท. ให้ความเห็นชอบในการแต่งตั้งนั้นแล้ว และให้สถาบันการเงินแจ้งการแต่งตั้งบุคคลที่ได้รับความเห็นชอบต่อ ธปท. ทราบภายใน 15 วัน นับแต่วันที่แต่งตั้งด้วย

[26] ในกรณีที่กรรมการ ผู้จัดการ รองผู้จัดการ หรือผู้ช่วยผู้จัดการ หรือที่ปรึกษาของสถาบันการเงิน ลาออก เสียชีวิต หรือการเปลี่ยนแปลงหน้าที่ในตำแหน่งงานระดับเดียวกัน ให้สถาบันการเงินแจ้งการเปลี่ยนแปลงดังกล่าวให้ ธปท. ทรายภายใน 15 วันนับแต่วันที่มีการเปลี่ยนแปลง

ทางการ คำสั่งของธนาคารแห่งประเทศไทย และระเบียบหรือข้อบังคับภายในของสถาบันการเงิน[27] คือ การจัดโครงสร้างการบริหารงานให้เป็นไปตามหลักการบริหารความเสี่ยง (risk-based approach) เพื่อให้เป็นไปตามวัตถุประสงค์ดังกล่าวจึงมีการนำ “หลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defense: 3LoD)”[28] ซึ่งเป็นกลไกการถ่วงดุลและดูแลให้มีการควบคุม กำกับ และตรวจสอบความเสี่ยง[29] ตลอดจนตรวจสอบการปฏิบัติงานมาใช้กันอย่างแพร่หลายในสถาบันการเงินไทย[30] เพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปตามกฎหมาย กฎระเบียบข้อบังคับต่างๆ ของทางการ คำสั่งการของธนาคารแห่งประเทศไทย สถาบันการเงินจะต้องจัดให้มีการแบ่งหน้าที่ความรับผิดชอบตามหลักการดังกล่าวให้ชัดเจน[31] เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

สถาบันการเงินควรกำหนดนโยบายในการกำกับดูแลข้อมูลส่วนบุคคล ให้สอดคล้องกับขนาด ลักษณะ การดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของสถาบัน

---

[27] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 10/2561 เรื่อง ธรรมภิบาลของสถาบันการเงิน

[28] การใช้คำว่าหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับนั้นไม่ได้มุ่งหวังที่จะแสดงองค์ประกอบในเชิงโครงสร้าง แต่เป็นการแยกแยะบทบาทหน้าที่อย่างมีประโยชน์ ตามหลักแล้วผู้บริหารระดับสูง (Senior Management) และคณะกรรมการ (Governing Body/Board/Audit Committee) ยังเป็นผู้มีหน้าที่กำกับดูแลด้วยแต่ไม่ได้ถูกจัดให้อยู่ในกลุ่มงานระดับใดระดับหนึ่งในสามระดับ ดังนั้น การให้ระดับหมายเลขจึงไม่ควรนำมาใช้เพื่อตีความว่าเป็นการปฏิบัติงานตามลำดับขั้น แท้จริงแล้วบทบาทหน้าที่ทั้งหมดจะทำงานไปพร้อมๆ กัน

[29] ตลาดหลักทรัพย์แห่งประเทศไทย, "กรอบการบริหารความเสี่ยงองค์กร (ERM Framework)" [ออนไลน์] เข้าถึงเมื่อ 20 ตุลาคม 2563. แหล่งที่มา: https://www.set.or.th/th/about/overview/files/Risk_2015_v2.pdf ความเสี่ยงของสถาบันการเงินอาจเป็นความเสี่ยงทางด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงทางด้านปฏิบัติการ (Operational Risk) หรือความเสี่ยงทางด้านกฎหมายและข้อกำหนดผูกพันองค์กร (Compliance Risk) นอกจากนี้ความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลก็เป็นความเสี่ยงทางกฎหมายอย่างหนึ่งที่สถาบันการต้องนำมาพิจารณาในปัจจุบันเช่นเดียวกัน

[30] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 10/2561 เรื่อง ธรรมาภิบาลของสถาบันการเงิน

[31] อนึ่ง ในสถาบันการเงินขนาดเล็กมักมีข้อจำกัดในการจัดวางโครงสร้างองค์กรให้เป็นไปตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ ทางออกที่เป็นไปได้ในการดำเนินงาน คือ การทำให้หน้าที่ความรับผิดชอบสำคัญที่มีโอกาสเกิดความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์ ต้องมีการปฏิบัติงานแบบคู่ขนาน (Dual Assignment) ไม่ใช่คนใดคนหนึ่งกระทำการเบ็ดเสร็จ เช่น การร่วมลงนาม 2 คน การเพิ่มขั้นตอนการสอบทานก่อนดำเนินการ การออกแบบเอกสารแบบฟอร์มให้ผ่านทุกหน่วยงานที่เกี่ยวข้องในชุดเดียวกันตั้งแต่ต้นจนจบกระบวนการ การตั้งคณะทำงานปฏิบัติงานแทนหน่วยงานตามหน้าที่ภายใต้โครงสร้าง เป็นต้น

การเงิน รวมถึงสื่อสารนโยบายดังกล่าวเพื่อสร้างความตระหนักแก่พนักงานในองค์กร รวมทั้งให้พนักงานถือปฏิบัติตาม หนึ่งในเรื่องที่สำคัญของนโยบายการกำกับดูแลข้อมูล คือ โครงสร้างการกำกับดูแลข้อมูล ซึ่งกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องให้เป็นไปตามหลักการ Three Lines of Defense และมีการแบ่งแยกหน้าที่อย่างชัดเจน ดังภาพด้านล่างนี้[32]

ตารางที่ 2 เปรียบเทียบความแตกต่างระหว่างบทบาทหน้าที่ของกลุ่มงานในแต่ละระดับตามหลักการ Three Lines of Defense

Management Functions		Assurance
1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Operating Management	Limited Independence Reports Primarily to Mgmt.	Internal Audit Greater Independence Reports to Governing Body

ที่มา: COSO. LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE. p.10.

กลุ่มงานระดับที่หนึ่ง (1st Line of Defense)

กลุ่มงานระดับที่หนึ่ง หมายถึง ฝ่ายงานผู้ปฏิบัติงาน (operational management) หรือหน่วยธุรกิจ (business unit)[33] ซึ่งรับผิดชอบควบคุมการบริหารและดำเนินงานในพันธกิจหลักที่สร้างรายได้หรือดำเนินงานตามวัตถุประสงค์หลักอื่นๆ ของกิจการ กลุ่มงานระดับแรกยังมีหน้าที่โดยตรงในการจัดการและควบคุมความเสี่ยงที่เกิดจากงานลักษณะของกิจกรรมแต่ละวัน (day-to-day basis) อันเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล มิให้ความเสี่ยงกระทบต่อเป้าหมายทางธุรกิจและวัตถุประสงค์ขององค์กร รวมทั้งทำหน้าที่ติดตามดูแลและรายงานความเสี่ยงและรายงานความเสียหายมายังฝ่ายบริหารความเสี่ยงเพื่อวิเคราะห์ผลกระทบในภาพรวมต่อสถาบันการเงิน

[32] COSO, LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE (The Institute of Internal Auditors (IIA), 2015). p.10.

[33] The Institution of Internal Auditors, "IAA Position Paper - The Three Lines of Defense in Effective Risk Management and Control," [Online] Accessed: 11 Mar 2021. Available from: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

ทั้งนี้ กลุ่มงานระดับที่หนึ่งอาจกำหนดแนวทางการจัดการเพิ่มเติมในส่วนที่เป็นวิธีการดำเนินงาน ขั้นตอนรายละเอียด (how to do) และแทรกกิจกรรมการควบคุมความเสี่ยงไว้ในระหว่างการปฏิบัติงานตามปกติ และในคำแนะนำการทำงาน (work Instruction) สำหรับบุคลากรในความรับผิดชอบของตนได้[34]

กลุ่มงานระดับที่สอง (2nd Line of Defense)

กลุ่มงานระดับที่สอง หมายถึง ฝ่ายงานบริหารความเสี่ยงและฝ่ายงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (Risk Management and Compliance Function) ทำหน้าที่กำกับความเสี่ยงโดยรวมที่เป็นผลมาจากการจัดการความเสี่ยงของแต่ละหน่วยงาน และให้ช่วยเหลือด้านการบริหารความเสี่ยงดังกล่าว โดยการออกแบบจัดวางกรอบแนวทางการจัดการความเสี่ยงให้กลุ่มงานระดับที่หนึ่งนำไปใช้งานจริง[35] ฝ่ายงานในกลุ่มงานระดับที่สอง เช่น ฝ่ายบริหารความเสี่ยง ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ หรือผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer: CISO)[36] เป็นต้น

ลักษณะและรูปแบบการดำเนินงานของกลุ่มงานระดับที่สองมีความเป็นอิสระจากกลุ่มงานระดับที่หนึ่งพอสมควร โดยไม่เข้าไปดำเนินการแก้ไขหรือจัดการความเสี่ยงต่างๆ แทนกลุ่มงานระดับที่หนึ่งด้วยตนเอง แต่จะส่งต่อให้กลุ่มงานระดับที่หนึ่งต้องจัดการความเสี่ยงและการกำกับ

[34] ibid.

[35] ibid. เนื่องจากลำพังการรับผิดชอบในการจัดการความเสี่ยงต่างๆ และความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์แต่เพียงลำพังของกลุ่มงานระดับที่หนึ่ง (1st Line) ยังไม่เพียงพอที่จะให้หลักประกันประสิทธิภาพของการจัดการความเสี่ยงที่จำกัดเฉพาะรายภาระงานได้ จึงต้องมีการกำกับชั้นที่สองจากกลุ่มงานที่ทำหน้าที่ออกแบบกำหนดกรอบแนวทางการจัดการความเสี่ยงและการกำกับการปฏิบัติตามกฎเกณฑ์ที่ใช้ประเมินผลสถานะความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์ในภาพรวมของกิจการ (Risk Oversight) เพื่อประเมินในภาพรวมของกิจการได้ว่าการจัดการความเสี่ยงของแต่ละฝ่ายงานอย่างเพียงพอ เหมาะสม และมีประสิทธิผลหรือไม่ หากพบว่าการจัดการของกลุ่มงานระดับที่หนึ่งส่วนใดยังไม่เพียงพอ ก็จะต้องพัฒนาและปรับปรุงการจัดการความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์ในส่วนนั้นเพิ่มเติม

[36] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

การปฏิบัติตามกฎเกณฑ์นั้นต่อไป หรือผู้บริหารระดับสูงอาจเข้าแทรกแซงด้วยการสั่งการให้เพิ่มเติม ปรับปรุง แก้ไขการจัดการความเสี่ยงและการกำกับการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์เองโดยตรงกับกลุ่มงานระดับที่หนึ่งโดยผ่านทางกลุ่มงานระดับที่สอง ซึ่งหน้าที่ความรับผิดชอบหลักของกลุ่มงานระดับที่สอง (2nd Line) อาจจะครอบคลุมถึง[37]

- สนับสนุนการดำเนินงานให้เป็นไปตามนโยบาย ด้วยการกำหนดระเบียบปฏิบัติในด้านการจัดการความเสี่ยงและในด้านการกำกับการปฏิบัติตามกฎเกณฑ์ให้แต่ละหน่วยงาน
- กำหนดกรอบแนวทาง วิธีระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง การจัดการความเสี่ยง และการกำกับการปฏิบัติตามกฎเกณฑ์ ตามสภาพแวดล้อมการดำเนินงานและสภาพแวดล้อมภายนอกกิจการ
- ระบุความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่ยังหลงเหลือในภาพรวมและความเสี่ยงจากกฎเกณฑ์ที่เกิดใหม่
- กำหนดแนวปฏิบัติหรือหลักสูตรการอบรมที่ลดช่องว่างเชิงสมรรถนะในการจัดการความเสี่ยงให้กับบุคลากร
- สร้างโครงสร้างพื้นฐาน สิ่งอำนวยความสะดวกในการจัดการความเสี่ยง และตรวจสอบการจัดการความเสี่ยงของฝ่ายงานผู้ปฏิบัติงาน
- แจ้งเตือนล่วงหน้าให้แก่กลุ่มงานระดับที่หนึ่งทราบในความเสี่ยงด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกิดใหม่
- ติดตาม วัดผลตามมาตรวัด และประเมินประสิทธิผลของการควบคุมความเสี่ยงและการปฏิบัติตามกฎเกณฑ์

<u>กลุ่มงานระดับที่สาม (3rd Line of Defense)</u>

[37] The Institution of Internal Auditors, "IAA Position Paper - The Three Lines of Defense in Effective Risk Management and Control." Ibid. pp.4-5.

กลุ่มงานระดับที่สาม หมายถึง หน่วยงานตรวจสอบภายใน (Internal Audit) เป็นกลุ่มงานที่ไม่ได้เกี่ยวข้องกับการปฏิบัติภาระงาน หรือดำเนินงานตามพันธกิจประจำ แต่ทำหน้าที่ในการตรวจสอบ สอบทาน หรือทดสอบว่าการปฏิบัติงานของหน่วยงานต่างๆ ภายในองค์กรเป็นไปตามหลักการบริหารความเสี่ยงหรือการกำกับการปฏิบัติงานเป็นไปตามกฎเกณฑ์อย่างแท้จริง[38] แต่กลุ่มงานระดับที่สามมีหน้าที่ให้การรับรองประสิทธิผลของการประเมินความเสี่ยงและประสิทธิผลของการบริหารความเสี่ยงของสถาบันการเงิน สร้างความเชื่อมั่นว่าองค์กรมีมาตรการบริหารความเสี่ยงเพียงพอและเหมาะสม[39] ซึ่งบทบาทหน้าที่ของกลุ่มงานระดับที่สาม (3rd Line) ครอบคลุมถึง[40]

- อิงตามมาตรฐานการตรวจสอบภายใน หรือคู่มือการปฏิบัติงานของคณะทำงาน/คณะกรรมการ
- รายงานการดำเนินงานต่อผู้บริหารระดับสูงและคณะกรรมการของสถาบันการเงิน
- ส่งต่อข้อมูลรายงานที่เป็นจุดอ่อนของการควบคุมให้กลุ่มงานระดับที่หนึ่งและกลุ่มงานระดับที่สอง เพื่อปรับปรุง แก้ไข หรือพัฒนาเพิ่มเติม

[38] FERMA-ECIIA, "GDPR & Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation," [Online] Accessed: 12 Oct 2020. Available from: https://www.ferma.eu/advocacy/gdpr-corporate-governance-the-role-of-internal-audit-and-risk-management-one-year-after-implementation/. Ibid. pp.5-6.

[39] กลุ่มงานมาตรฐานด้านการตรวจสอบภายใน, "แนวปฏิบัติการตรวจสอบภายใน" [ออนไลน์] เข้าถึงเมื่อ 21 ตุลาคม 2563. แหล่งที่มา: http://www.khonkaen.go.th/auditor/admin/interest_file/102127_536.pdf (ฝ่ายงานตรวจสอบภายในต้องตรวจสอบกิจกรรมของสถาบันการเงินหลากหลายด้าน เช่น การตรวจสอบดำเนินงาน (Operational auditing) การตรวจสอบผลการปฏิบัติงาน (Performance auditing) การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance auditing) การตรวจสอบทางการเงิน (Financial Auditing) หลักฐานที่องค์กรนั้นอ้างว่าได้ดำเนินงานอย่างถูกต้อง (Attestation) รวมไปถึงการตรวจสอบสารสนเทศ (Information Technology Auditing) ว่าระบบงานและข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ของสถาบันการเงินรวมทั้งระบบการเข้าถึงข้อมูลในการปรับปรุงแก้ไขและการรักษาความปลอดภัยของข้อมูลมีความถูกต้องและเชื่อถือได้)

[40] FERMA-ECIIA, "Guidance on the 8th EU Company Law Directive - Article 41," [Online] Accessed: 13 Mar 2021. Available from: https://www.iia.nl/SiteFiles/ECIIA%20FERMA.pdf

ในประเทศไทยได้นำเรื่องการแบ่งแยกบทบาทหน้าที่ตามหลักการ Three Lines of Defense มาใช้กำหนดโครงสร้างการกำกับดูแลองค์กร (Corporate Governance) อย่างแพร่หลาย โดยเฉพาะอย่างยิ่งในการกำกับดูแลข้อมูล (Data Governance) ของสถาบันการเงิน ดังนี้ต่อไปนี้[41]

ตารางที่ 3 บทบาทหน้าที่และความรับผิดชอบตามหลักการ Three Lines of Defense ที่เกี่ยวกับการกำกับดูแลข้อมูลในสถาบันการเงิน

บทบาทหน้าที่และความรับผิดชอบที่เกี่ยวกับการกำกับดูแลข้อมูล	
1. คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล	Oversight Committee
2. ผู้บริหารจัดการข้อมูล 2.1 ระดับผู้บริหารระดับสูง 2.2 ระดับหน่วยงานหรือทีมงาน	1st Line
3. ผู้อนุมัติการดำเนินการต่างๆ ที่เกี่ยวกับข้อมูล	
4. ผู้ใช้ข้อมูล	
5. หน่วยงานบริหารความเสี่ยง	2nd Line
6. หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์และกฎหมาย	
7. หน่วยงานตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวกับข้อมูล	3rd Line

ที่มา: แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance)

1. คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล[42] มีหน้าที่
   - บริหารจัดการข้อมูล ให้เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
   - ส่งเสริมการให้ความรู้ และสร้างความตระหนักแก่บุคลากรทั่วทั้งองค์กร

[41] แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance), 27 กันยายน 2564

[42] คณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูล สามารถประกอบด้วยผู้บริหารที่เกี่ยวข้อง เช่น ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer) ผู้บริหารระดับสูงด้านบริหารจัดการข้อมูล (Chief Data Officer) ผู้บริหารระดับสูงด้านการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Chief Information Security Officer) ผู้บริหารระดับสูงด้านความเสี่ยง (Chief Risk Officer) หรือผู้บริหารจากส่วนงานอื่นที่เกี่ยวข้อง

2. ผู้บริหารจัดการข้อมูล ทั้งระดับผู้บริหารระดับสูง และระดับหน่วยงานหรือทีมงาน

   2.1 ระดับผู้บริหารระดับสูง มีหน้าที่

   - บริหารจัดการข้อมูล ให้เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
   - ส่งเสริมการให้ความรู้ และสร้างความตระหนักแก่บุคลากรทั่วทั้งองค์กร

   2.2 ระดับหน่วยงานหรือทีมงาน มีหน้าที่

   - จัดทำทบทวน ปรับปรุงนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูลให้เป็นปัจจุบัน
   - สื่อสาร ให้ความรู้ และให้คำแนะนำเกี่ยวกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติ
   - เกี่ยวข้องกับการกำกับดูแลข้อมูล รวมทั้ง การสร้างความตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายในองค์กร
   - ติดตามสถานะของการบริหารจัดการข้อมูล รายงาน ผลและประเด็นปัญหาหรือความเสี่ยงที่พบต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลข้อมูลเป็นประจำ

3. ผู้อนุมัติการดำเนินการต่างๆ ที่เกี่ยวกับข้อมูล มีหน้าที่

   - อนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล เช่น อนุญาตการเข้าถึงข้อมูล การใช้และเผยแพร่ข้อมูล
   - ควบคุมดูแลข้อมูลให้มั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐานและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล เช่น ดูแลให้จัดทำทะเบียนข้อมูลและทบทวนให้เป็นปัจจุบัน ดูแลให้มีการกำหนดชั้นความลับข้อมูลและกำหนดเกณฑ์คุณภาพข้อมูล

4. ผู้ใช้ข้อมูล มีหน้าที่

- ปฏิบัติตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล
- สนับสนุนการกำกับดูแลข้อมูลให้ตรงความต้องการในการใช้ข้อมูล และรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลไปยังหน่วยงานหรือทีมงานที่ทำหน้าที่บริหารจัดการข้อมูล

5. หน่วยงานบริหารความเสี่ยง มีหน้าที่
   - จัดทำกรอบและกระบวนการบริหารความเสี่ยงของสถาบันการเงินให้ครอบคลุมความเสี่ยงด้านข้อมูล รวมทั้งสนับสนุนให้หน่วยงานต่างๆ มีการประเมินความเสี่ยงด้านข้อมูล
   - ให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวมและเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่นของสถาบันการเงิน และนำเสนอผล การบริหารจัดการความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง
6. หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์และกฎหมาย มีหน้าที่
   - ติดตาม ให้คำปรึกษา และกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลเพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องกับข้อมูลของหน่วยงานกำกับดูแล
7. หน่วยงานตรวจสอบ มีหน้าที่
   - ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลเพื่อสอบทานให้มั่นใจว่าเป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

การจัดโครงสร้างองค์กรของสถาบันการเงินตามแนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance) ข้างต้นสอดคล้องกับหลักการของ Federation of European Risk Management Associations (FERMA)[43] ที่ได้ให้คำแนะนำเกี่ยวกับแนวทางใน

[43] FERMA-ECIIA, "GDPR & Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation."

การกำหนดตำแหน่งภายในองค์กรของ DPO (position of DPO) โดยกำหนดให้ DPO ต้องปฏิบัติหน้าที่ด้วยความเป็นกลาง มีอิสระจากผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล และไม่มีอำนาจตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการการประมวลผลข้อมูลส่วนบุคคล

โดย FERMA เห็นว่า[44] การแบ่งแยกบทบาทหน้าที่ DPO ออกจากฝ่ายงานสารสนเทศ (IT) เป็นสิ่งที่จำเป็นในการรับรองว่ากลยุทธ์ในการบริหารความเสี่ยงด้านไซเบอร์นั้นสอดคล้องกับกลยุทธ์และวัตถุประสงค์ในการดำเนินธุรกิจขององค์กร ตลอดจนแนะนำว่า DPO ควรจะอยู่ในกลุ่มงานระดับที่สอง (2nd Line of Defense) เนื่องจากเป็นบุคคลผู้ให้คำแนะนำและตรวจสอบการดำเนินงานให้ฝ่ายงานต่างๆ ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไม่เช่นนั้นจะทำให้ความเป็นอิสระในการตัดสินใจปฏิบัติงาน (independent manner) ไม่สามารถเกิดขึ้นได้[45]

อย่างไรก็ตาม เนื่องจากไม่มีกฎหมายใดบังคับให้ DPO ต้องมาจากสายงานใดหรือบังคับให้มีใบประกอบวิชาชีพทางด้านใด ในทางปฏิบัติสถาบันการเงินจึงสามารถแต่งตั้ง DPO จากกลุ่มงานอื่นๆ ที่ไม่ใช่กลุ่มงานระดับที่สองได้เช่นกัน

2) บุคคลภายนอก (Outsource)

ถึงแม้ว่า DPO อาจเป็นลูกจ้างหรือพนักงานของสถาบันการเงินที่มีหน้าที่อื่นในองค์กรได้ก็ตาม[46] แต่เป็นที่ทราบกันดีว่าการแต่งตั้งบุคคลภายในสถาบันการเงินอาจทำให้เกิดปัญหาความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO ขึ้นได้ เนื่องจากลูกจ้างหรือพนักงานของสถาบันการเงินไม่ว่าจะเป็นบุคคลที่ทำงานเต็มเวลา (full-time) หรือทำงานเป็นกะเวลา (part-time) มักจะต้องปฏิบัติตามคำสั่งผู้บริหารของสถาบันการเงิน อีกทั้งไม่มีอำนาจในการบริหารจัดการงบประมาณของตนเอง[47] นอกจากนี้การแต่งตั้งบุคคลภายในมีความเป็นไปได้ที่จะเกิดการขัดกันแห่งผลประโยชน์

---

[44] ibid.

[45] GDPR, Recital 97

[46] GDPR, Recital 97

[47] Douwe Korff and Marie Georges, "The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation.". pp.135-136.

(conflict of interest) หรือการขัดกันในบทบาทหน้าที่ (conflict of duties) เนื่องจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีส่วนร่วมในการดำเนินงานของสถาบันการเงินอย่างใกล้ชิด และมีตำแหน่งสูงพอที่จะมีอำนาจตัดสินใจด้านข้อมูลส่วนบุคคล เช่น เป็นผู้บริหารระดับสูง (senior management level) หรือเป็นบุคคลอื่นใดที่มีอำนาจตัดสินใจต่อการประมวลผลข้อมูลส่วนบุคคล ดังนั้น อีกทางเลือกหนึ่งของสถาบันการเงิน คือ การเลือกแต่งตั้ง DPO เป็นบุคคลภายนอกองค์กร

การที่สถาบันการเงินแต่งตั้ง DPO เป็นบุคคลภายนอกต้องพิจารณาหลักเกณฑ์ตามประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ในการพิจารณาว่าหากสถาบันการเงินต้องการแต่งตั้ง DPO เป็นผู้ให้บริการภายนอกมีหลักเกณฑ์การคัดเลือกเบื้องต้นเป็นอย่างไรนั้น จะต้องพิจารณาประเด็นสำคัญก่อนที่จะทำสัญญาใหม่หรือทบทวนเพื่อต่ออายุสัญญาการใช้บริการจากผู้ให้บริการภายนอกรายเดิม[48] อย่างน้อย ดังต่อไปนี้

1) ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ และประสบการณ์ในการดำเนินงาน
2) สถานะความมั่นคงทางการเงิน
3) ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียน หรือถูกฟ้องร้องดำเนินคดี
4) วัฒนธรรมองค์กรและนโยบายการให้บริการที่มีความเหมาะสมกับสถาบันการเงิน
5) ความสามารถในการปรับตัวตอบสนองพัฒนาการใหม่ๆ
6) ความเสี่ยงในกรณีที่ผู้ให้บริการภายนอกให้บริการแก่สถาบันการเงินหลายแห่ง (Concentration Risk)
7) หลักเกณฑ์ที่ชัดเจนเกี่ยวกับการพิจารณาการใช้บริการจากผู้ให้บริการภายนอกที่มีส่วนเกี่ยวข้องกับคณะกรรมการและผู้บริหารระดับสูง

สำหรับการพิจารณาว่าการใช้ผู้ให้บริการภายนอกเป็น DPO ของสถาบันการเงินมีหลักเกณฑ์ในการอนุญาตอย่างไรจะต้องพิจารณาว่าการปฏิบัติงานของ DPO เป็นงานของสถาบัน

[48] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

การเงินในลักษณะใดตามประกาศฯ เมื่อ DPO มีหน้าที่หลักในการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและให้คำแนะนำต่อองค์กร เพื่อป้องกันมิให้การประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินก่อให้เกิดความเสียหายต่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 42 จะเห็นได้ว่าการปฏิบัติงานของ DPO มีลักษณะเป็นงานหลักที่ไม่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ (Non-strategic function)[49] เนื่องจากเป็นงานที่มีความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลของลูกค้า ข้อมูลและสินทรัพย์ของสถาบันการเงิน และการปฏิบัติตามหลักเกณฑ์ของทางการ และถึงแม้การปฏิบัติหน้าที่ของ DPO อาจกระทบต่อฐานะการดำเนินงานและความเสี่ยงของสถาบันการเงินอยู่บ้าง แต่ก็ถูกจัดว่าเป็นความเสี่ยงในระดับหนึ่งเท่านั้น ประกอบกับงานของ DPO ไม่ใช่งานที่เกี่ยวข้องกับการตัดสินใจหรือการทำธุรกรรมใดที่กระทบต่อสถาบันการเงินโดยตรง งานของ DPO จึงมิใช่งานหลักที่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ ซึ่ง ธปท. ไม่อนุญาตให้สถาบันการเงินใช้บริการจากผู้ให้การภายนอกแต่อย่างใด

โดยงานหลักไม่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ (Non-strategic function) มีหลักเกณฑ์การอนุญาตการใช้บริการจากผู้ให้บริการภายนอก ดังต่อไปนี้

[49] งานหลักที่ไม่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ (Non-strategic function) หมายถึง งานที่มีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(1) งานจัดหาหรือวิเคราะห์ข้อมูลเบื้องต้นเพื่อประกอบการตัดสินใจ

(2) งานที่มีความเสี่ยงในระดับหนึ่ง เนื่องจากเกี่ยวข้องกับข้อมูลส่วนบุคคลของลูกค้า ข้อมูลและสินทรัพย์ของสถาบันการเงิน รวมถึงการปฏิบัติตามหลักเกณฑ์ของทางการ

(3) งานที่มีข้อกังวลในเรื่องความเสี่ยงหากมีการใช้บริการจากผู้ให้บริการภายนอกในต่างประเทศ

ตามเอกสารแนบ 1 ของประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 ได้ยกตัวอย่างงานหลักที่เกี่ยวข้องกับการตัดสินใจเชิงกลยุทธ์ เช่น งานวิเคราะห์สินเชื่อเบื้องต้น งานนำข้อมูลส่วนบุคคลของลูกค้าเข้าระบบงานประเมินมูลค่าพอร์ต (กำไร/ขาดทุน) งานพัฒนาโมเดลความเสี่ยงและการทดสอบความถูกต้องแม่นยำของโมเดล งานตรวจสอบหรือสอบทานกระบวนการบริหารความเสี่ยง (Risk Management Process) ที่ต้องใช้ความเชี่ยวชาญเฉพาะด้าน งาน Detect Fraud ที่เกี่ยวกับความเสี่ยงด้านปฏิบัติการ งานจัดทำบัญชีและการเงิน งานด้านการกำกับดูแลการปฏิบัติตามกฎหมาย (Compliance) งานตรวจสอบภายใน (Internal Audit) เป็นต้น

1. หากผู้ให้บริการภายนอกที่อยู่ในประเทศไทย ธปท. อนุญาตให้สถาบันการเงินแต่ละแห่งสามารถใช้บริการจากผู้ให้บริการภายนอกที่อยู่ในประเทศไทยได้เป็นการทั่วไป
2. หากผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ เนื่องจากการใช้ DPO ซึ่งเป็นผู้ให้บริการภายนอกที่อยู่ในต่างประเทศมีองค์ประกอบความเสี่ยงที่แตกต่างจากการใช้ DPO ซึ่งเป็นผู้ให้บริการภายนอกที่อยู่ในประเทศไทย[50] เช่น ความเสี่ยงจากการเปลี่ยนแปลงหรือความไม่แน่นอนทางเศรษฐกิจ การเมือง สังคม และกฎหมายของผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ ความซับซ้อนในการบริการความต่อเนื่องทางธุรกิจที่อยู่ในต่างประเทศ การบังคับใช้ตามกฎหมายระหว่างประเทศหรือกฎหมายประเทศนั้นๆ เป็นต้น ประกอบกับข้อจำกัดในทางกฎหมายในการกำกับดูแลแบบรวมกลุ่ม (Consolidated Supervision) ซึ่ง ธปท. ไม่มีอำนาจในการกำกับดูแลบริษัทที่มีความเกี่ยวข้องของสถาบันการเงินที่เป็นบริษัทลูกหรือเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ จึงมีการกำหนดเงื่อนไขการอนุญาตสำหรับสถาบันการเงินประเภทดังกล่าวแตกต่างจากสถาบันการเงินไทย ดังนี้
   - กรณีสถาบันการเงินไทย ไม่รวมถึงธนาคารพาณิชย์ไทยที่มีต่างชาติถือหุ้นมากกว่ากึ่งหนึ่ง (Hybrid bank) ให้สถาบันการเงินขออนุญาตธนาคารแห่งประเทศไทยก่อนการใช้ DPO ซึ่งเป็นผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ เฉพาะกรณีที่ผู้ให้บริการภายนอกนั้นไม่ใช่บริษัทในกลุ่มธุรกิจเดียวกัน

[50] ตามประกาศของธนาคารแห่งประเทศไทยที่ สนส. 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน สรุปความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกไว้ 9 หมวด ได้แก่ ความเสี่ยงด้านกลยุทธ์ (Strategy Risk) ความเสี่ยงด้านชื่อเสียง (Reputation Risk) ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Compliance Risk) ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงด้านคู่สัญญา (Counterparty Risk) ความเสี่ยงจากสภาวะแวดล้อมในแต่ละประเทศ (Country Risk) ความเสี่ยงด้านสัญญาและข้อตกลง (Contractual Risk) ความเสี่ยงที่สถาบันการเงินไม่อาจเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Access Risk) ความเสี่ยงที่เกิดจากการกระจุกตัวและผลกระทบต่อระบบสถาบันการเงินโดยรวม (Concentration and Systemic Risk) เป็นต้น

- กรณีธนาคารพาณิชย์ไทยที่มีต่างชาติถือหุ้นมากกว่ากึ่งหนึ่ง (Hybrid bank) หรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ (Subsidiary) หรือเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ ให้สถาบันการเงินขออนุญาตธนาคารแห่งประเทศไทยก่อนการใช้ DPO ซึ่งเป็นผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ ทั้งในกรณีที่ผู้ให้บริการภายนอกเป็นบริษัทในกลุ่มธุรกิจเดียวและไม่ใช่บริษัทในกลุ่มธุรกิจเดียวกัน

ตารางที่ 4 หลักเกณฑ์การอนุญาตการใช้ DPO จากผู้ให้บริการภายนอกตามประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 (Outsourcing)

ประเภทของสถาบันการเงิน	ผู้ให้บริการภายนอกที่อยู่ในประเทศไทย		ผู้ให้บริการภายนอกที่อยู่ในต่างประเทศ	
	บริษัทในกลุ่ม	บริษัทนอกกลุ่ม	บริษัทในกลุ่ม	บริษัทนอกกลุ่ม
สถาบันการเงินไทย ไม่รวม Hybrid bank	✓	✓	✓	*
Hybrid bank / Subsidiary	✓	✓	*	*
สาขาของธนาคารพาณิชย์ต่างประเทศ	-	✓	-	*
หมายเหตุ: ✓ อนุญาตเป็นการทั่วไป * ต้องขออนุญาตก่อนดำเนินการ				

ที่มา: ประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน, หน้า.6

หากสถาบันการเงินได้รับอนุญาตให้ใช้ DPO เป็นผู้ให้บริการภายนอกแล้ว และภายหลังมีการเปลี่ยนแปลงหรือเพิ่มเติมผู้ให้บริการภายนอก หรือผู้ให้บริการมอบหมายหรือว่าจ้างผู้ให้บริการภายนอกรายอื่นรับช่วงงานต่อ (subcontract) บางส่วนหรือทั้งหมดของงานที่รับจ้างมา

สถาบันการเงินไม่ต้องยื่นขออนุญาตใหม่ เว้นแต่กรณีที่มีการเปลี่ยนแปลงประเภทของผู้ให้บริการภายนอกที่เข้าข่ายต้องขออนุญาตธนาคารแห่งประเทศไทย[51] ตามตารางข้างต้น

ทั้งนี้ ตามประกาศของธนาคารแห่งประเทศไทยฯ ไม่ว่าจะเป็นกรณีอนุญาตเป็นการทั่วไปหรือกำหนดให้สถาบันการเงินต้องยื่นขออนุญาตการใช้ DPO ซึ่งเป็นผู้ให้บริการภายนอกต่อ ธปท. สถาบันการเงินมีบทบาทในการติดตามข้อมูลการใช้บริการจากผู้ให้บริการภายนอก รวมทั้งประเมินแนวทางควบคุมและบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก ดังนี้

- สถาบันการเงินมีหน้าที่ต้องรายงานข้อมูลเกี่ยวกับ DPO ซึ่งเป็นผู้ให้บริการภายนอก[52] ต่อ ธปท. เป็นประจำทุกปี ปีละ 1 ครั้ง
- สถาบันการเงินมีหน้าที่จัดทำแบบประเมินแนวทางและประสิทธิภาพของการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการภายนอกในภาพรวมเป็นประจำทุกปี ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการภายนอกอย่างมีนัยสำคัญ และจัดเก็บผลการประเมินไว้ที่สถาบันการเงิน โดยจะต้องสามารถจัดส่งให้ ธปท. ได้เมื่อร้องขอ

2.1.2 แต่งตั้งโดยพิจารณาจากความสามารถของ DPO

บทบาทหน้าที่หลักของ DPO คือการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินให้เป็นไปตามกฎหมายและให้คำแนะนำที่เหมาะสมแก่องค์กร รวมถึงอาจต้องติดต่อกับเจ้าของข้อมูลส่วนบุคคลและประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับดูแลในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูล[53] DPO จึงต้องมีความสามารถ (Competency) อย่างน้อย 3 ด้าน

---

[51] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน ข้อ 5.4.2

[52] สถาบันการเงินต้องรายงานข้อมูลการใช้บริการจากผู้ให้บริการภายนอก ได้แก่ ชื่องาน ชื่อผู้ให้บริการภายนอก ประเภทของผู้ให้บริการภายนอก (มีความเกี่ยวข้องกับผู้ให้บริการภายนอกเป็นบริษัทในหรือนอกกลุ่มธุรกิจการเงินหรือไม่) สถานที่ตั้งของผู้ให้บริการภายนอก และรายละเอียดเพิ่มเติม (ถ้ามี)

[53] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42

ได้แก่ ความรู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ความเข้าใจรูปแบบการประมวลผลข้อมูลส่วนบุคคลของธุรกิจสถาบันการเงินสถาบันการเงิน และความรู้ทางด้านเทคโนโลยีสารสนเทศซึ่งใช้ในระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคลในสถาบันการเงิน นอกจากนี้ DPO ของสถาบันการเงินควรมีความรู้ความเข้าใจด้านอื่นประกอบด้วย เพื่อให้สามารถทำหน้าที่ตรวจสอบและให้คำแนะนำต่อองค์กรได้ดียิ่งขึ้น ทั้งนี้แล้วแต่ความเหมาะสมของแต่ละสถาบันการเงิน (โดยผู้เขียนจะกล่าวถึงความรู้ความเข้าใจเหล่านั้นต่อไปใน “หัวข้อ 4.2 ความรู้ความเข้าใจ”)

ฉะนั้น สถาบันการเงินอาจแต่งตั้ง DPO โดยพิจารณาตามความรู้ความสามารถส่วนบุคคลของบุคคลที่จะเข้ามารับตำแหน่ง DPO ก็ได้ ซึ่งแบ่งเป็นบุคคลประเภทต่างๆ ดังต่อไปนี้

1. <u>บุคคลคนเดียว</u>

ในกรณีที่สถาบันการเงินมีความจำเป็นที่จะต้องตรวจสอบและให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลอยู่ในระดับที่ต่ำ หรือองค์กรมีขนาดเล็กซึ่งจำนวนการประมวลผลข้อมูลส่วนบุคคลน้อยและการเก็บ รวบรวม ใช้ข้อมูลส่วนบุคคลนั้นมีความเรียบง่ายไม่ซับซ้อนยุ่งยากมากนัก สถาบันการเงินอาจกำหนดให้บุคคลคนเดียวทำหน้าที่เป็น DPO ได้

2. <u>ทีมงาน</u>

เนื่องจาก DPO จำเป็นต้องมีความรู้ความเข้าใจหลากหลายด้าน โดยอย่างน้อย ได้แก่ ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ด้านรูปแบบการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงิน และด้านเทคโนโลยีสารสนเทศซึ่งใช้ในระบบรักษาความปลอดภัยของข้อมูลส่วนบุคคล (ผู้เขียนจะกล่าวถึงความรู้ความเข้าใจด้านอื่นที่จำเป็นต่อการปฏิบัติหน้าที่ DPO ต่อไปในบทที่ 4) ในทางปฏิบัติจึงเป็นไปได้ยากที่บุคคลคนเดียวจะสามารถมีความรู้ความเข้าใจรอบด้าน และอาจจำเป็นต้องมีการแต่งตั้ง DPO หลายคน[54] [55] หรืออาจตั้งเป็นคณะทำงานด้านการคุ้มครองข้อมูล

[54] การแต่งตั้ง DPO ขององค์กรหลายคนอาจมีประโยชน์ต่อการแบ่งเบาภาระงานและประโยชน์ในด้านความรู้ความสามารถ แต่ก็อาจก่อให้เกิดปัญหาอำนาจการตัดสินใจขึ้นได้ในกรณีที่ DPO แต่ละคนมีความคิดเห็นไม่ตรงกัน

ส่วนบุคคล (data protection office) เพื่อทำหน้าที่สนับสนุน DPO เพียงคนเดียว ก็เป็นอีกทางหนึ่งที่สถาบันการเงินสามารถทำได้

2.2 สภาพปัญหาของ DPO ในสถาบันการเงิน

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 DPO มีหน้าที่หลักคือการตรวจสอบและให้คำแนะนำเพื่อให้กระบวนการประมวลผลข้อมูลส่วนบุคคลขององค์กรเป็นไปตามกฎหมาย แต่เนื่องจากสำหรับประเทศไทยกฎหมายเรื่องดังกล่าวมีความใหม่อยู่มาก และไม่เคยมีมาตรฐานหรือกฎเกณฑ์ที่ให้ความสำคัญกับหลักการทั่วไปของการคุ้มครองข้อมูลส่วนบุคคล[56] โดยเฉพาะอย่างยิ่งในส่วนของ DPO ซึ่งเป็นบุคคลสำคัญต่อการทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลสัมฤทธิ์ผลได้จริงในทางปฏิบัติ ประกอบกับการที่ พ.ร.บ. ดังกล่าวเพียงแต่กำหนดหลักเกณฑ์ในเรื่องกรณีที่หน่วยงานต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานะของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้อย่างกว้าง อีกความคืบหน้าของกฎหมายลำดับรองที่กำหนดรายละเอียดในเรื่องข้างต้นก็ยังอยู่ในขั้นตอนของร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งไม่ได้ลงรายละเอียดเกี่ยวกับโครงสร้างการปฏิบัติงานที่เหมาะสมแก่ DPO ความรู้ความสามารถหรือระบบการรับรองคุณวุฒิที่เกี่ยวข้อง เพราะอาจต้องรอกฎหมายมีผลใช้บังคับไปสักระยะหนึ่งแล้วจึงจัดการรับฟังความเห็นของ DPO ผู้ปฏิบัติงานจริงว่าเกิดปัญหาในเรื่องใดบ้าง จึงทำให้เกิดปัญหาในการกำหนดตัวบุคคลที่จะทำหน้าที่เป็น DPO ในสถาบันการเงินทั้งปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงิน (Organizational) และปัญหาเชิง

---

[55] ปัจจุบันมีร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.9 ทำให้องค์กรไม่สามารถแต่งตั้งให้นิติบุคคลเป็น DPO ได้ (โดยรายละเอียดผู้เขียนได้กล่าวไว้แล้วใน “หัวข้อ 4.6.1 การรับรองคุณสมบัติของ DPO”)

[56] ก่อนหน้าการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประเทศไทยมีกฎหมายสำคัญที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นการคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานใดหน่วยงานหนึ่งหรือธุรกิจใดธุรกิจหนึ่งเป็นการเฉพาะเจาะจง คือ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 โดยอ้างอิงหลักการคุ้มครองข้อมูลส่วนบุคคลต่างๆ ตาม The OECD Privacy Principles แต่ยังไม่เคยมีกฎหมายที่เป็นหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคลหรือบุคคลผู้ทำหน้าที่เช่นเดียวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแต่อย่างใด

ความสามารถของตัวเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Competency) ตลอดจนปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน (Implementation)

ภาพที่ 4 สภาพปัญหาของ DPO ในสถาบันการเงิน

ประการแรก ปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงิน (Organizational) เป็นปัญหาที่ส่งผลโดยตรงต่อความรับผิดทางกฎหมายของสถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เช่น

- ปัญหาการมีส่วนเกี่ยวข้องภายในสถาบันการเงิน เนื่องจาก DPO จะต้องทำหน้าที่ตรวจสอบและให้คำแนะนำ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีส่วนเกี่ยวข้องในทุกประเด็นที่สัมพันธ์กับการคุ้มครองข้อมูลส่วนบุคคลด้วยวิธีการที่เหมาะสมและทันท่วงที[57] สถาบันการเงินควรกำหนดกระบวนการปรึกษาหารือระหว่างฝ่ายงานกับ DPO ไว้ในลักษณะใด DPO ต้องมีบทบาทในการทบทวนและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามหลักการทั่วไปของกฎหมายการคุ้มครองข้อมูลส่วนบุคคล (GDPR Principles) อย่างไร เป็นต้น
- ปัญหาเกี่ยวกับทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย ด้วยเหตุที่กฎหมายกำหนดหน้าที่ให้สถาบันการเงินสนับสนุนการปฏิบัติภารกิจและหน้าที่ของ DPO โดยการจัดหาทรัพยากรที่จำเป็นในการปฏิบัติภารกิจและการเข้าถึงข้อมูลส่วนบุคคล[58] แต่

[57] GDPR, Article 38(1)

[58] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสอง บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่” และ Article 38(2) of GDPR กำหนดว่าผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

กฎหมายขาดความชัดเจน และไม่มีแนวปฏิบัติใดระบุว่าทรัพยากรดังกล่าวหมายถึงอะไรบ้าง ซึ่งความต้องการทางด้านทรัพยากรของ DPO ในสถาบันการเงินอาจมีความแตกต่างไปจากภาคธุรกิจหรือองค์กรอื่นในประเทศไทย

- ปัญหาความเป็นอิสระในการตัดสินใจปฏิบัติงาน ด้วยสาเหตุที่กฎหมายกำหนดให้สถาบันการเงินต้องรับรองถึงความเป็นอิสระในการปฏิบัติหน้าที่ (Independence)[59] ของ DPO จึงเกิดปัญหาขึ้นว่า DPO ควรจะจะดำรงตำแหน่งอยู่ในส่วนใดหรือฝ่ายใดของสถาบันการเงิน มีสายการบังคับบัญชาและสายการรายงานอย่างไร ประเด็นใดบ้างที่ต้องมีการรายงาน นอกจากนี้กฎหมายยังกำหนดรับรองตำแหน่งหน้าที่ของบุคคลที่เป็น DPO โดย DPO จะถูกปลด เลิกสัญญาหรือลงโทษจากการที่ตนปฏิบัติหน้าที่หรือภารกิจตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้[60] แต่ควรจะมีกลไกประการอื่นที่ช่วยรับรองความเป็นอิสระของ DPO ได้อีกหรือไม่ โดยเฉพาะอย่างยิ่งหากเกิดกรณีที่สถาบันการเงินปลด DPO ที่ปฏิบัติหน้าที่อย่างถูกต้องตามกฎหมายออกจากตำแหน่งและอ้างเหตุผลอย่างอื่นเพื่อหลีกเลี่ยงความรับผิดทางกฎหมาย
- ปัญหาความขัดแย้งทางผลประโยชน์ หาก DPO ของสถาบันการเงินมีหน้าที่หรือภารกิจอย่างอื่นต่อองค์กร การปฏิบัติหน้าที่เหล่านั้นต้องไม่ก่อให้เกิดความขัดแย้งทางผลประโยชน์ (Conflict of Interest) ระหว่างหน้าที่ภายในสถาบันการเงินและหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล[61] กรณีใดบ้างที่ถือว่าเข้าข่ายความขัดแย้งทางผลประโยชน์ ควรมีกระบวนการป้องกันไม่ให้เกิดกรณีดังกล่าวอย่างไร และเป็นประเด็นปัญหานี้มีความสัมพันธ์กับปัญหาความเป็นอิสระในการตัดสินใจปฏิบัติงาน

จะต้องสนับสนุนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการปฏิบัติภารกิจตาม Article 39 โดยการจัดหาทรัพยากรที่จำเป็นเพื่อการปฏิบัติภารกิจเหล่านั้นและการเข้าถึงข้อมูลส่วนบุคคล การเข้าถึงการปฏิบัติการประมวลผลข้อมูลส่วนบุคคล และเพื่อยืนยันถึงความรู้ในระดับสูงของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล”

[59] ทั้งตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสาม และ Article 38(3), GDPR ต่างก็ได้มีการบัญญัติรับรองความเป็นอิสระของ DPO ไว้ในลักษณะเดียวกันว่า ผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องรับรองว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถปฏิบัติหน้าที่ได้โดยไม่ได้รับคำแนะนำใดๆ ในประเด็นที่เกี่ยวข้องกับการปฏิบัติภารกิจเหล่านั้น และ DPO ต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

[60] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรค 3 และ GDPR, Article 38(3)

[61] พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสี่ และ GDPR, Article 38(6)

ประการที่สอง ปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน (Competency) เป็นปัญหาที่มีความสำคัญต่อประสิทธิผลให้คำแนะนำ และการตรวจสอบกระบวนการประมวลผลข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมาย เช่น

- ปัญหาความรู้ความเข้าใจ เนื่องจากลักษณะการปฏิบัติงานของ DPO ต้องทราบว่ารูปแบบธุรกิจและการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินเป็นอย่างไร สถาบันการเงินมีความจำเป็นในการจัดเก็บข้อมูลอย่างไร มากน้อยเพียงใด ภายในสถาบันการเงินมีการไหลเวียนของข้อมูลอย่างไร รวมถึงต้องมีความเข้าใจด้านเทคโนโลยีสารสนเทศ (IT) และมาตรฐานความปลอดภัยของข้อมูลประกอบด้วย เพราะในปัจจุบันมีการใช้เทคโนโลยีสารสนเทศในการพัฒนาระบบรักษาความปลอดภัยของข้อมูลของสถาบันการเงินอย่างแพร่หลาย DPO ของสถาบันการเงินจึงไม่ใช่จะเป็นบุคคลใดก็ได้แต่ต้องมีประสบการณ์ วิชาชีพ ความรู้ความเชี่ยวชาญและทักษะหลากหลายด้าน อย่างไรก็ดี กฎหมายแทบไม่ได้กำหนดรายละเอียดในเรื่องดังกล่าวหรือยังขาดความชัดเจนอยู่มาก
- การรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล และการรับรองคุณวุฒิ (Accreditation and Certification) เนื่องจากการอบรมเกี่ยวกับการปฏิบัติงานของ DPO ในประเทศไทยขาดการรับรองที่ชัดเจน หรืออาจกล่าวได้ว่าอยู่ระหว่างการพัฒนายังไม่อยู่ในระดับที่ได้มาตรฐานเมื่อเปรียบเทียบกับหลักสูตรของต่างประเทศ ประกอบกับหลักสูตรการฝึกอบรมและใบรับรองคุณวุฒิอาจมีความแตกต่างกันในแต่ละองค์กรได้

ประการที่สาม ปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน (Implementation) เป็นปัญหาที่พนักงาน เจ้าหน้าที่ หรือบุคคลในคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้ง DPO ต้องเผชิญในการดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งส่วนใหญ่มีสาเหตุมาจากความไม่ชัดเจนของกฎหมายและขาดแนวปฏิบัติงานที่เพียงพอ เช่น การสนับสนุนจากผู้บริหารระดับสูง (Tone from the Top) การประกาศแจ้งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) การเก็บรักษาและลบข้อมูลส่วนบุคคล (Data Retention) การจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data

Processing Agreement) หรือ การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer) เป็นต้น

วิทยานิพนธ์ฉบับนี้ ผู้เขียนจะทำการสัมภาษณ์ DPO และคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงผู้ที่เกี่ยวข้องอื่นในแต่ละสถาบันการเงินในประเทศไทย โดยเน้นไปที่ธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจ ผู้เขียนคาดว่าจะทำให้ทราบว่าสถาบันการเงินแต่ละแห่งเลือกแต่งตั้งบุคคลใดให้ปฏิบัติหน้าที่ในตำแหน่ง DPO มีโครงสร้างการกำกับดูแลหรือมาตรการในการส่งเสริมให้ DPO มีส่วนร่วมในทุกประเด็นที่เกี่ยวกับข้อมูลส่วนบุคคล มีความเป็นอิสระในการตัดสินใจทำงาน และอยู่ในสถานะที่ปราศจากความขัดแย้งทางผลประโยชน์ได้อย่างไร DPO ของสถาบันการเงินควรจะเป็นผู้ที่มีความรู้ความสามารถในด้านใดบ้าง ตลอดจนประสบปัญหาใดจากการปฏิบัติหน้าที่ตามกฎหมายและจากการปฏิบัติหน้าที่ต่อองค์กรหรือไม่ อะไรบ้าง

โดยในบทที่ 3 และบทที่ 4 จะกล่าวถึงปัญหาเชิงโครงสร้างองค์กร (Organizational) และปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน (Competency) และทำการศึกษาต่อไปในบทที่ 5 เกี่ยวกับปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน (Implementation) เพื่อหาแนวทางและข้อเสนอแนะในการแก้ไขปัญหาทางปฏิบัติเกี่ยวกับตำแหน่ง DPO ในสถาบันการเงิน

บทที่ 3

ปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงิน

ในการแต่งตั้ง DPO ขึ้นมาทำหน้าที่กำกับดูแลกิจกรรมการประมวลผลของสถาบันการเงินให้เป็นไปตามมาตรฐานสากลและข้อบังคับของกฎหมาย สถาบันการเงินจะต้องคำนึงถึงข้อพิจารณาต่างๆ ที่ใช้ในการกำหนดบุคคลผู้ที่มาทำหน้าที่เป็น DPO ขององค์กร หนึ่งในข้อพิจารณาดังกล่าว คือ ข้อพิจารณาทางด้านความสัมพันธ์ระหว่าง DPO กับสถาบันการเงินที่มีการแต่งตั้ง ซึ่งตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่างก็ได้กำหนดความสัมพันธ์ระหว่าง DPO กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลของสถาบันการเงินซึ่งอยู่ในบทบัญญัติเรื่องเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายในองค์กรไว้ในลักษณะเดียวกัน เช่น องค์กรที่มีหน้าที่ในการแต่งตั้ง DPO[1] การมีส่วนเกี่ยวข้องกับประเด็นการคุ้มครองข้อมูลส่วนบุคคลของ DPO[2] หน้าที่การสนับสนุนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ DPO[3] การรับรองความเป็นอิสระในการปฏิบัติหน้าที่[4] หน้าที่ในการรักษาความลับที่ได้ล่วงรู้มาจากการปฏิบัติหน้าที่ DPO[5] หรือการปราศจากความขัดแย้งทางผลประโยชน์ (Conflict of interest)[6] เป็นต้น ในทางปฏิบัติ DPO จึงต้องมีส่วนในการสร้างสภาพแวดล้อมที่ดีต่อการทำงานขององค์กร รักษาความสัมพันธ์ระหว่างนายจ้างและลูกจ้าง หรือระหว่างผู้บังคับบัญชากับผู้อยู่ใต้บังคับบัญชา ไปพร้อมๆ กับให้คำแนะและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมายอย่างเหมาะสม

---

[1] GDPR, Article 37 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41

[2] GDPR, Article 38(1)

[3] GDPR, Article 38(2) และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสอง

[4] GDPR, Article 38(3) และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสาม

[5] GDPR, Article 38(5) และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(4)

[6] GDPR, Article 38(6) และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคท้าย

European Data Protection Supervisor (EDPS) อธิบายถึงประเด็นเกี่ยวกับโครงสร้างองค์กรที่อาจส่งผลกระทบต่อความเหมาะสมของการปฏิบัติหน้าที่ให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ DPO ซึ่งประเด็นดังกล่าวสามารถแบ่งแยกพิจารณาออกได้เป็น 6 ข้อ ดังนี้[7]

ภาพที่ 5 ประเด็นเกี่ยวกับโครงสร้างองค์กรที่มีผลต่อการปฏิบัติหน้าที่ DPO

ตามตารางข้างต้น ประเด็นเกี่ยวกับโครงสร้างองค์กรที่ส่งผลต่อความเหมาะสมแก่การปฏิบัติหน้าที่ DPO ได้แก่ (1) การมีส่วนเกี่ยวข้องภายในองค์กร (2) ทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ (3) ความเป็นอิสระ (4) ความขัดแย้งทางผลประโยชน์ (5) ระยะเวลา และการพ้นจากตำแหน่งของ DPO และ (6) สถานะของผู้ช่วย DPO (Assistant DPO) และผู้แทน DPO (Acting DPO) โดยปัจจัยเหล่านี้ล้วนมีความเกี่ยวข้องกับความสัมพันธ์ระหว่าง DPO กับสถาบันการเงินที่เป็นผู้แต่งตั้ง

สำหรับการศึกษาปัญหาเชิงโครงสร้างองค์กรของสถาบันการเงินในบทนี้ ผู้เขียนได้เลือกศึกษาโดยใช้วิธีการเก็บแบบสอบถามและการสัมภาษณ์เชิงลึก DPO และบุคคลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของแต่ละสถาบันการเงิน จำนวน 12 แห่ง รวมถึงของธนาคารแห่งประเทศไทย รวมทั้งสิ้น 13 แห่ง ระหว่างเดือนมิถุนายน ปี พ.ศ. 2564 ถึงเดือนสิงหาคม ปี พ.ศ. 2564 ซึ่งจำแนกตาม

[7] EDPS, "Position paper on the role of Data Protection Officers of the EU institutions and bodies," [Online] Accessed: 16 Jan 2021. Available from: https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf, pp.7-12.

ประเภท ขนาด และสถานภาพขององค์กร เพื่อให้ข้อมูลครบถ้วน อันประกอบด้วย ธนาคารพาณิชย์จดทะเบียนในประเทศไทย[8] จำนวน 8 แห่ง (แบ่งออกเป็นธนาคารพาณิชย์ขนาดใหญ่ 4 แห่ง ธนาคารพาณิชย์ขนาดกลาง 1 แห่ง และธนาคารพาณิชย์ขนาดเล็ก 3 แห่ง) และสถาบันการเงินเฉพาะกิจ (SFI) จำนวน 4 แห่ง (แบ่งออกเป็นสถาบันการเงินเฉพาะกิจขนาดกลาง 1 แห่ง และสถาบันการเงินเฉพาะกิจขนาดเล็ก 3 แห่ง) ซึ่งต่อไปนี้ผู้เขียนจะเรียกว่า “บทสัมภาษณ์ กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง” โดยพบว่าสถาบันการเงินแต่ละแห่งล้วนแต่งตั้งจากบุคลากรภายในองค์กร (in-house) เป็น DPO

ตารางที่ 5 ข้อมูลเบื้องต้นของผู้ให้สัมภาษณ์ (ข้อมูล ณ เดือนสิงหาคม 2564)

สถาบันการเงินขนาดใหญ่[9]		
ชื่อสถาบันการเงิน	ประเภท	ฝ่ายของ DPO
1. ธนาคารกรุงเทพ จำกัด (มหาชน)	ธนาคารพาณิชย์	กฎหมาย (ไม่เป็นทางการ)
2. ธนาคารกรุงไทย จำกัด (มหาชน)	ธนาคารพาณิชย์	Compliance
3. ธนาคารไทยพาณิชย์ จำกัด (มหาชน)	ธนาคารพาณิชย์	IT
4. ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)	ธนาคารพาณิชย์	Compliance
สถาบันการเงินขนาดกลาง[10]		
5. ธนาคารอาคารสงเคราะห์	สถาบันการเงินเฉพาะกิจ	ผู้ตรวจการธนาคาร
6. ธนาคารยูโอบี จำกัด (มหาชน)	ธนาคารพาณิชย์	กฎหมาย
สถาบันการเงินขนาดเล็ก[11]		
7. ธนาคารซีไอเอ็มบี ไทย จำกัด (มหาชน)	ธนาคารพาณิชย์	กำกับดูแลข้อมูล
8. ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)	ธนาคารพาณิชย์	กฎหมาย
9. ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน)	ธนาคารพาณิชย์	กฎหมาย

[8] ธนาคารพาณิชย์จดทะเบียนในประเทศไทย ไม่รวมธนาคารพาณิชย์เพื่อรายย่อยและธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารต่างประเทศ

[9] สถาบันการเงินขนาดใหญ่ ประกอบด้วยสถาบันการเงินที่มีส่วนแบ่งตลาดของสินทรัพย์รวมตั้งแต่ร้อยละ 10 ขึ้นไป (เมื่อเทียบกับสินทรัพย์รวมธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยทั้งระบบ)

[10] สถาบันการเงินขนาดกลาง ประกอบด้วยสถาบันการเงินที่มีส่วนแบ่งตลาดของสินทรัพย์รวมตั้งแต่ร้อยละ 2.5 แต่ไม่ถึงร้อยละ 10 (เมื่อเทียบกับสินทรัพย์รวมธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยทั้งระบบ)

[11] สถาบันการเงินขนาดเล็ก ประกอบด้วยสถาบันการเงินที่มีส่วนแบ่งตลาดของสินทรัพย์รวมต่ำกว่าร้อยละ 2.5 (เมื่อเทียบกับสินทรัพย์รวมธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยทั้งระบบ)

10. ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย (EXIM)	สถาบันการเงินเฉพาะกิจ	Compliance
11. บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม	สถาบันการเงินเฉพาะกิจ	IT
12. ธนาคารอิสลามแห่งประเทศไทย	สถาบันการเงินเฉพาะกิจ	IT
ธนาคารกลาง		
13. ธนาคารแห่งประเทศไทย	ธนาคารกลาง	บริหารความเสี่ยง

3.1 การมีส่วนเกี่ยวข้องภายในสถาบันการเงินของ DPO

สถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลต้องรับรองว่า DPO จะมีส่วนเกี่ยวข้องในทุกประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรอย่างเหมาะสมและทันท่วงที[12] หลักกฎหมายนี้มีวัตถุประสงค์เพื่อให้แน่ใจว่า DPO จะได้รับข้อมูลที่เพียงพอต่อการปฏิบัติหน้าที่ตามกฎหมาย และสามารถให้คำปรึกษาตั้งแต่ขั้นตอนแรกของแต่ละกิจกรรมการประมวลผลข้อมูลตามหลักการคุ้มครองความเป็นส่วนตัวตั้งแต่การออกแบบ (Privacy by Design)[13] อันจะทำให้แนวคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลเข้ามาเป็นส่วนหนึ่งของวัฒนธรรมการทำงานองค์กรอย่างแท้จริง

หลักการ Privacy by Design ส่งผลให้ DPO ของแต่ละสถาบันการเงินมีส่วนร่วมในการออกแบบการดำเนินงานครบวงจรชีวิตข้อมูล (data life cycle) โดยไม่เป็นการขัดขวางการปฏิบัติหน้าที่ขององค์กร เมื่อสถาบันการเงินคำนึงความเป็นส่วนตัวเป็นส่วนหนึ่งตั้งแต่การออกแบบผลิตภัณฑ์ หรือการให้บริการแล้ว จะทำให้ข้อมูลส่วนบุคคลเกิดความปลอดภัยตั้งแต่เริ่มต้นจนจบกระบวนการ[14] โดยหลักการข้างต้นสามารถพิจารณาได้ 4 มิติ[15] ซึ่งแต่ละมิติล้วนมีความสำคัญต่อความโปร่งใสของการตรวจสอบข้อมูล (Accountability) และจำเป็นต้องมีการกำกับดูแลโดย DPO และหน่วยงานกำกับดูแล ได้แก่

[12] GDPR, Article 44(1)

[13] GDPR, Article 25

[14] EDPS, "Preliminary Opinion on privacy by design (Opinion 5/2018)," [Online] Accessed: 22 Oct 2021. Available from: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf. p.4 (para.17).

[15] Ibid, pp.6-7 (paras. 27-32).

1. องค์กรต้องจัดให้มีมาตรการป้องกันตั้งแต่ต้นในกระบวนการประมวลผลข้อมูลส่วนบุคคล
2. การประมวลผลข้อมูลส่วนบุคคลไม่ว่าแต่เพียงบางส่วนหรือทั้งหมดควรเป็นผลมาจากการออกแบบการคุ้มครองข้อมูลที่ครอบคลุมทั้งวงจรชีวิตของข้อมูล
3. กระบวนการออกแบบควรตั้งอยู่บนพื้นฐานการบริหารความเสี่ยง โดยจะต้องคำนึงถึงสิทธิและเสรีภาพของเจ้าของข้อมูลอยู่เสมอ
4. มาตรการที่ใช้คุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลจะต้องเหมาะสมและมีประสิทธิภาพ

กล่าวคือ เมื่อทำให้ DPO มาเข้ามีส่วนเกี่ยวข้องกับกระบวนการออกแบบมาตรการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลตั้งแต่เริ่มต้นตัดสินใจเลือกกระบวนการอย่างเป็นระบบ จะส่งผลให้แต่ละสถาบันการเงินสามารถปฏิบัติตามหลักการ Privacy by Design ได้ โดย DPO ของแต่ละสถาบันการเงินอาจมีส่วนเกี่ยวข้องได้หลากหลายรูปแบบ เช่น เข้าประชุมกับผู้บริหารระดับสูงและระดับกลางอย่างสม่ำเสมอ[16] มีส่วนร่วมในการให้คำแนะนำและควบคุมดูแลการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล ให้คำแนะนำในการจัดทำ DPIA จัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การดูแลและให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล หรือมีส่วนร่วมในการบริหารจัดการเหตุรั่วไหลทั้งกระบวนการตั้งแต่ต้น เป็นต้น

3.1.1 กระบวนการปรึกษาหารือกับฝ่ายที่ประสงค์จะใช้ข้อมูล

เพื่อให้กระบวนการดำเนินงานของสถาบันการเงินมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมครบทั้งวงจรชีวิตข้อมูล ในความเป็นจริงฝ่ายงานภายในองค์กรที่ประสงค์จะใช้ข้อมูลส่วนบุคคลควรขอคำปรึกษาจาก DPO ก่อนการใช้ข้อมูล โดยเฉพาะอย่างยิ่งหากการใช้ข้อมูลนั้นมีความเสี่ยงสูงที่อาจกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล DPO มีหน้าที่ให้คำแนะนำและให้คำปรึกษาด้านการปฏิบัติการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร หรือประเด็นต่างๆ

---

[16] Article 29 Data Protection Working Party (WP29), "Guidelines on Data Protection Officers (‘DPOs’)," [Online] Accessed: 20 Jan 2021. Available from: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A. p.13.

เกี่ยวกับกฎระเบียบด้านการคุ้มครองข้อมูลส่วนบุคคล[17] เพื่อให้เป็นไปตามกฎหมายหรือมาตรการที่เกี่ยวข้องซึ่งอาจมีการเปลี่ยนแปลงตลอดเวลา และให้คำแนะนำแก่ผู้บริหารและผู้ปฏิบัติงานภายในองค์กรทราบถึงกฎระเบียบใหม่ๆ แนวปฏิบัติ มาตรการ คำพิพากษา ข้อแนะนำที่ออกโดยรัฐบาล รวมถึงแนวทางคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ[18]

แต่ละสถาบันการเงินจึงควรออกนโยบาย กฎระเบียบ หรือข้อบังคับใดๆ ที่เป็นการกำหนดกระบวนการปรึกษาหารือระหว่าง DPO กับฝ่ายงานที่ประสงค์จะใช้ข้อมูลไว้อย่างชัดเจน และจัดให้มีการบันทึกการให้คำปรึกษาหารือแต่ละครั้งเป็นหลักฐานเพื่อให้คำปรึกษาที่ DPO ให้ไว้สำหรับแต่ละฝ่ายงานมีความสอดคล้องและเป็นไปในทางเดียวกัน นอกจากนี้การจัดให้มีบันทึกการให้คำปรึกษาหารือจะเป็นประโยชน์เมื่อหน่วยงานกำกับดูแล เช่น ธปท. หรือ สคส. เข้ามาตรวจสอบสถาบันการเงินและการปฏิบัติหน้าที่ของ DPO

การนี้ ผู้เขียนจึงได้ทำการเก็บข้อมูลจากแบบสอบถาม และการสัมภาษณ์เชิงลึก DPO และผู้ที่เกี่ยวข้องของสถาบันการเงินแต่ละแห่ง จำนวน 13 แห่ง ซึ่งผู้เขียนได้แบ่งประเด็นคำถามเกี่ยวกับกระบวนการปรึกษาหารือระหว่าง DPO กับฝ่ายงานภายในองค์กรที่ประสงค์จะใช้ข้อมูลออกเป็น 3 ข้อ ได้แก่ (1) การกำหนดกระบวนการภายในองค์กร (2) ประเด็นการให้คำปรึกษาและแสดงความเห็น และ (3) การจัดทำบันทึกการให้คำปรึกษาหารือ

(1) การกำหนดกระบวนการภายในองค์กร

DPO ควรเข้ามามีส่วนร่วมให้คำปรึกษาหรือคำแนะนำ อย่างน้อยในขั้นตอนต่างๆ ได้แก่ การจัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เมื่อเกิดเหตุต้องสงสัยว่าอาจเป็นการละเมิดข้อมูลส่วนบุคคล (Data breach) รวมถึงการตรวจสอบการดำเนินงานของลูกจ้างหรือผู้รับจ้างของสถาบันการเงินใน

---

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42(1)

[18] Douwe Korff and Marie Georges, "The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation.". p.230

การปฏิบัติตามกฎหมาย[19] นอกจากนี้ สถาบันการเงินแต่ละแห่งต้องกำหนดบทบาทหน้าที่ของ DPO ไว้อย่างชัดเจนถึง อำนาจในการตรวจสอบของ DPO และความถี่ของการตรวจสอบ[20]

ผู้เขียนได้สัมภาษณ์ DPO รวมถึงผู้ที่อยู่ในคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของแต่ละสถาบันการเงินว่า “สถาบันการเงินของท่านมีการกำหนดกระบวนการปรึกษาหารือกับ DPO อย่างชัดเจนหรือไม่ มีความครอบคลุมงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างไรบ้าง” พบว่ามีทั้งสถาบันการเงินที่มีการกำหนดกระบวนการปรึกษาหารือกับ DPO (7 แห่ง) และสถาบันการเงินที่อยู่ในระหว่างดำเนินการ (2 แห่ง) รวมถึงสถาบันการเงินที่เห็นว่าสามารถใช้กระบวนการของฝ่ายงานเดิมที่มีอยู่ (4 แห่ง) ปรากฏตามตารางดังต่อไปนี้

ตารางที่ 6 สถาบันการเงินที่มีกระบวนการปรึกษาหารือระหว่างฝ่ายงานภายในองค์กรกับ DPO

การกำหนดกระบวนการปรึกษาหารือระหว่างฝ่ายงานกับ DPO	**ขนาดใหญ่**	**ขนาดกลาง**	**ขนาดเล็ก**
กำหนดกระบวนการ	2	1	4
ไม่ได้กำหนดกระบวนการไว้โดยเฉพาะ	3	1	-
อยู่ระหว่างกำหนดกระบวนการ	-	-	2

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ตามตารางข้างต้น การกำหนดกระบวนการปรึกษาหารือของสถาบันการเงินแต่ละแห่งระหว่าง DPO กับฝ่ายงานภายในองค์กรนั้นมีลักษณะที่แตกต่างกัน โดยสามารถสรุปได้ดังตารางด้านล่างดังนี้

[19] ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, "สัมภาษณ์ เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล,"(29 กรกฎาคม 2564).

[20] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดียวกัน

ภาพที่ 6 ลักษณะการกำหนดกระบวนการปรึกษาหารือกับ DPO ของสถาบันการเงิน

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า สถาบันการเงินที่ได้กำหนดกระบวนการปรึกษาหารือไว้อย่างชัดเจน (7 แห่ง) เกี่ยวกับ เรื่องที่จะต้องปรึกษาหารือหรือต้องขออนุมัติจาก DPO ก่อนดำเนินการใช้ข้อมูลส่วนบุคคล ซึ่งกระบวนการปรึกษาหารือระหว่าง DPO และหน่วยงานที่ประสงค์จะใช้ข้อมูลส่วนบุคคลจะมีความแตกต่างกันไปในแต่ละองค์กร โดยผู้เขียนหยิบยกการกำหนดกระบวนการปรึกษาหารือระหว่างฝ่ายที่ประสงค์จะใช้ข้อมูลส่วนบุคคลกับ DPO ที่สำคัญ ดังนี้[21]

สถาบันการเงินขนาดใหญ่แห่งหนึ่ง ได้กำหนดกระบวนการปรึกษาหารือระหว่างหน่วยงานภายในกับ DPO ซึ่งมีความครอบคลุมงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กร

[21] กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, "สัมภาษณ์ เรื่อง บทบาทหน้าที่และปัญหาที่เกิดขึ้นจากการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล,"(ระหว่างเดือนมิถุนายน - สิงหาคม 2564). ซึ่งหลังจากนี้จะเรียกว่า “บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง”

โดยแบ่งออกเป็น 2 เรื่อง คือ 1. เรื่องการจัดทำมาตรฐานแนวปฏิบัติ (Standard set-up) เช่น นโยบายความเป็นส่วนตัว ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล และการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และ 2. เรื่องการดำเนินการให้เป็นไปตามกฎหมาย (Implementation) แบ่งเป็นกรณีทั่วไป (ประชุมเดือนละ 2 ครั้ง) และกรณีมีความจำเป็นเร่งด่วน

สถาบันการเงินขนาดเล็กแห่งหนึ่ง กำหนดกระบวนการปรึกษาหารือกับ DPO ไว้อย่างชัดเจน โดยมีรายละเอียดอยู่ในคู่มือและแบบฟอร์มการปรึกษาหารือ เช่น รูปแบบการตอบ เอกสารที่ต้องใช้ประกอบการปรึกษาหารือ หมายเลขการตอบเพื่อความสะดวกเมื่อหน่วยงานกำกับดูแลเข้ามาตรวจสอบ ความคิดเห็นของ DPO ประจำฝ่ายงาน เป็นต้น ซึ่งต้องให้ความเห็นทุกกรณีที่มีข้อมูลส่วนบุคคล และมีความมั่นใจว่ากระบวนการปรึกษาหารือดังกล่าวครอบคลุมทุกงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพราะก่อนดำเนินการได้ทำการค้นหาช่องว่างทั้งหมดขององค์กร ทั้งช่องว่างของกิจกรรมและช่องของหลักเกณฑ์ต่างๆ

สถาบันการเงินขนาดเล็กอีกแห่งหนึ่ง มีการจัดตั้ง Data Protection Steering Committee (DPSC) ซึ่งประกอบด้วยผู้ประสานงานจากหน่วยธุรกิจต่างๆ เพื่อให้แต่ละฝ่ายงานมีศูนย์กลางในการปรึกษาหารือของฝ่ายงานเอง และจัดให้มีการประชุม DPSC เป็นรายเดือนเพื่อปรึกษาหารือและมอบหมายงาน

ในขณะที่ สถาบันการเงินที่มิได้กำหนดกระบวนการปรึกษาหารือไว้โดยเฉพาะ (4 แห่ง) เนื่องจากทางปฏิบัติสามารถขอคำปรึกษาจาก DPO หรือหน่วยงานที่มีอยู่แล้วซึ่งทำหน้าที่รับผิดชอบงานด้านการคุ้มครองข้อมูลส่วนบุคคลอีกเรื่องหนึ่งนอกเหนือจากภาระหน้าที่หลักผ่านช่องทางต่างๆ เช่น ทางโทรศัพท์ อีเมล์ หรือการประชุมหารือ ได้ให้เหตุผลที่สำคัญไว้ดังนี้[22]

ผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดใหญ่ กล่าวว่า “ในการปฏิบัติงานร่วมกันระหว่าง DPO Office กับหน่วยธุรกิจ ไม่มีการระบุเป็นรายกรณีว่าเรื่องใดต้องมาขอความเห็นหรือขออนุมัติ แต่ได้กำหนดให้มีการปรึกษาหารือทุกครั้งเมื่อมีผลิตภัณฑ์หรือการให้บริการใหม่ๆ ที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคล เริ่มต้นจากการประเมินความเสี่ยงของการประมวลผลข้อมูลผ่านกระบวนการที่มีอยู่ของธนาคาร ซึ่งต้องพิจารณาความเสี่ยงที่อาจกระทบต่อความเป็นส่วนตัวของ

[22] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดียวกัน

เจ้าของข้อมูลเพิ่มเติม หรือที่เรียกว่า DPIA แล้วแจ้งมายัง DPO Office เพื่อตรวจสอบผลการประเมินดังกล่าวอีกครั้งหนึ่ง”

เจ้าหน้าที่อาวุโสฝ่ายบริหารความเสี่ยงของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “องค์กรไม่ได้มีการกำหนดกระบวนการปรึกษาหารือกับ DPO อย่างเป็นลายลักษณ์อักษรชัดเจน แต่ได้กำหนดกรอบการดำเนินงาน (framework) เพื่อให้ส่วนงานต่างๆ จัดการข้อมูลได้ตามวัตถุประสงค์และเท่าที่จำเป็นตามกรอบระยะเวลาการจัดเก็บข้อมูล”

ส่วนผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่ง กล่าวว่า “ไม่มีการกำหนดกระบวนการเป็นเฉพาะ เนื่องจากฝ่ายงานต่างๆ สามารถขอคำปรึกษาจากฝ่าย Compliance ตามกระบวนการที่มีอยู่แล้ว ซึ่งเป็นฝ่ายที่รับผิดชอบการปฏิบัติตามกฎเกณฑ์ ไม่ว่าจะเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นๆ”

สำหรับสถาบันการเงินที่อยู่ระหว่างดำเนินการ (2 แห่ง) ได้ให้เหตุผลที่ยังไม่มีการกำหนดกระบวนการปรึกษาหารือดังกล่าว ดังต่อไปนี้[23]

DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่ง กล่าวว่า “ได้กำหนดนโยบายและมอบหมายให้ฝ่ายงานที่เกี่ยวข้องดำเนินการแล้ว แต่ยังไม่มีการกำหนดรายละเอียดว่ากรณีใดบ้างที่หน่วยงานภายในองค์กรต้องขอคำปรึกษาจาก DPO ก่อนการใช้ข้อมูลส่วนบุคคล เนื่องจากกฎหมายเลื่อนการบังคับใช้และปัจจุบันองค์กรกำลังให้ความสำคัญกับงานช่วยเหลือผู้ประกอบการที่ได้รับผลกระทบจากสถานการณ์โควิด-19 แต่ในทางปฏิบัติหน่วยงานต่างๆ สามารถขอคำปรึกษาหารือได้โดย ส่วนใหญ่เป็นเรื่องการประเมินความเสี่ยงของกิจกรรมการประมวลผลข้อมูล”

DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่ง กล่าวว่า “อยู่ระหว่างกำหนดกระบวนการ แม้จะยังไม่มีกระบวนการที่ชัดเจน แต่สามารถขอคำปรึกษาได้ โดยเรื่องที่ให้คำปรึกษาในช่วงไม่กี่เดือนที่ผ่านมา เช่น การเข้ารหัสข้อมูล (encryption) ซึ่งเกือบทุกกรณีที่ธนาคารส่งหรือโอนข้อมูลส่วนบุคคลได้ผ่านระบบที่ DPO เป็นผู้ดูแล”

[23] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดียวกัน

(2) ประเด็นการให้คำปรึกษาและแสดงความเห็น

ดังที่กล่าวในหัวข้อก่อนหน้า ประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานผู้ประสงค์จะใช้ข้อมูลควรขอคำปรึกษากับ DPO คือ การจัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล[24] การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)[25] [26] เหตุละเมิดข้อมูลส่วนบุคคล[27] และการตรวจสอบการดำเนินงานอื่นๆ ตามหน้าที่ของผู้ควบคุมข้อมูลที่กฎหมายกำหนด ดังนั้น เพื่อให้แน่ใจว่า DPO จะเข้ามามีบทบาทในการกำกับดูแลกระบวนการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินตั้งแต่ขั้นตอนแรกไปจนตลอดวงจรชีวิตข้อมูล สถาบันการเงินแต่ละแห่งควรกำหนดกฎระเบียบว่าผู้ควบคุมข้อมูลส่วนบุคคลจะต้องขอคำปรึกษาจาก DPO ในกรณีใดบ้าง ซึ่งกฎระเบียบนี้จะเป็นจุดเริ่มต้นและเป็นเครื่องมือส่งเสริมการมีส่วนร่วมของ DPO ภายในองค์กร[28]

---

[24] Douwe Korff, and Marie Georges. Ibid, p.235.

[25] WP29, Guidelines on DPOs. Ibid, p.17. (ปัจจุบันยังไม่มีการบัญญัติไว้ในกฎหมายไทยอย่างชัดแจ้ง ในขณะที่ GDPR, Article 35(2) กำหนดให้ DPO มีหน้าที่ที่ให้คำแนะนำในการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เช่น ควรจัดทำ DPIA หรือไม่ ใช้วิธีใด ให้บุคคลภายในองค์กรเป็นผู้ทำหรือว่าจ้างบุคคลภายนอก มีมาตรการใดในการบรรเทาจัดการความเสี่ยงทั้งทางเทคนิคและทางองค์กร DPIA ที่จัดทำขึ้นมีความถูกต้องสมบูรณ์ และความชอบด้วยกฎหมายหรือไม่ เป็นต้น)

[26] Article 29 Data Protection Working Party (WP29), "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." (ถึงแม้ DPO จะมีหน้าที่ให้คำแนะนำในการจัดทำ DPIA แก่ผู้ควบคุมข้อมูล โดยมิได้มีหน้าที่หรือส่วนร่วมในการประเมินความเสี่ยงโดยทั่วไป แต่ในทางปฏิบัตินั้น DPO ควรมีบทบาทในการประเมินความเสี่ยงโดยทั่วไปด้วย เพราะในหลายกรณีนั้นการประเมินความเสี่ยงขององค์การอาจต้องขอความเห็นจาก DPO ทั้งนี้ การประเมินความเสี่ยงดังกล่าวมีความหมายกว้างกว่าความเสี่ยงที่อาจกระทบต่อสิทธิในความเป็นส่วนตัว และสิทธิในการได้รับคุ้มครองข้อมูลส่วนบุคคล แต่รวมถึงความเสี่ยงต่อสิทธิและเสรีภาพขั้นพื้นฐานอื่นๆ เช่น เสรีภาพในการแสดงออก เสรีภาพในความคิด เสรีภาพในการเดินทาง เสรีภาพในการนับถือศาสนา การไม่ถูกเลือกปฏิบัติโดยไม่เป็นธรรม สิทธิทางประชาธิปไตย สิทธิที่จะไม่ถูกตรวจสอบจากทางรัฐเกินความจำเป็น สิทธิที่จะได้รับการเยียวยา เป็นต้น)

[27] WP29, Guidelines on DPOs. Ibid, p.14.

[28] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies, Ibid, p.8.

อย่างไรก็ดี ปัจจุบันกฎหมายไทยยังไม่ได้มีการกำหนดโดยชัดแจ้งว่ากรณีใดบ้างที่ผู้ควบคุมข้อมูลต้องขอคำปรึกษาจาก DPO ก่อนดำเนินการ หรือ DPO มีหน้าที่ให้คำปรึกษาในประเด็นใดบ้าง ในการนี้ ผู้เขียนจึงได้สอบถามว่าที่ผ่านมา DPO และบุคคลในคณะทำงานคุ้มครองข้อมูลของแต่ละสถาบันการเงินจำนวน 13 แห่ง มีโอกาสให้คำปรึกษากับสถาบันการเงินในเรื่องใดบ้าง ประมาณกี่ครั้ง โดยแบ่งประเด็นที่ให้คำปรึกษาออกเป็น (1) การจัดทำแนวปฏิบัติและคู่มือการทำงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (2) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และ (3) เหตุที่อาจเข้าข่ายละเมิดข้อมูลส่วนบุคคล รวมถึงประเด็นอื่นๆ ถ้ามี ซึ่งจากการสัมภาษณ์พบว่าที่ผ่านมาจำนวนของการให้คำปรึกษาในแต่ละประเด็นการคุ้มครองข้อมูลส่วนบุคคลของ DPO โดยเฉลี่ย ปรากฏดังตารางต่อไปนี้[29]

ตารางที่ 7 จำนวนครั้งโดยเฉลี่ยของประเด็นที่ DPO ให้คำปรึกษา

ประเด็นที่ให้คำปรึกษาหารือ	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
การจัดทำแนวปฏิบัติ คู่มือการทำงาน	134 ครั้ง	10 ครั้ง	9 ครั้ง
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	9 ครั้ง	2 ครั้ง	11 ครั้ง
เหตุการณ์ที่อาจเข้าข่ายละเมิดข้อมูลส่วนบุคคล	4 ครั้ง	2 ครั้ง	3 ครั้ง
คำขอใช้สิทธิของเจ้าของข้อมูล	13 ครั้ง/เดือน	ไม่มีข้อมูล	6 ครั้ง/เดือน
ข้อซักถามปลีกย่อยอื่นๆ	26 ครั้ง/เดือน	23 ครั้ง/เดือน	7 ครั้ง/เดือน

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

โดยประเด็นการคุ้มครองข้อมูลส่วนบุคคลในแต่ละเรื่องข้างต้นของสถาบันการเงินแต่ละแห่ง มีรายละเอียดของการให้คำปรึกษาหารือหรือการให้คำแนะนำในลักษณะดังนี้[30]

[29] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[30] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 8 ประเด็นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ DPO ให้คำปรึกษา

ประเด็นที่ให้คำปรึกษา	คำอธิบาย
การจัดทำแนวปฏิบัติ คู่มือการทำงาน	ก่อนการจัดทำ DPO ของสถาบันการเงินต่างๆ ได้ปรึกษากับบริษัทที่ปรึกษากฎหมาย ผู้เชี่ยวชาญ รวมถึงอาจารย์มหาวิทยาลัยต่างๆ และจัดประชุมรับฟังความเห็นของแต่ละส่วนงานภายในองค์กร โดยปัจจุบันอยู่ระหว่างรอความชัดเจนของกฎหมายลำดับรอง เพื่อปรับปรุงแนวปฏิบัติและคู่มือการทำงานต่อไป
การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	เนื่องจากความไม่ชัดเจนของเกณฑ์ในการประเมินระดับความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล สถาบันการเงินแต่ละแห่งจึงต้องศึกษาวิธีการทำจากแนวปฏิบัติปฏิบัติของภาคธุรกิจธนาคารโดยสมาคมธนาคารไทย หรือแนวปฏิบัติของคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย (TDPG) รวมถึงแนวปฏิบัติที่เกี่ยวข้องของต่างประเทศ เป็นต้น โดย DPO มีหน้าที่ให้คำแนะนำแก่ฝ่ายบริหารความเสี่ยงซึ่งเป็นผู้รับผิดชอบ
เหตุการณ์ที่อาจเข้าข่ายละเมิดข้อมูลส่วนบุคคล	ที่ผ่านมาเป็นพบเพียงแต่เหตุที่ต้องสงสัยว่าเป็นการละเมิดข้อมูลส่วนบุคคล แต่เมื่อพิจารณาแล้วปรากฏว่าไม่ใช่การละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ.ฯ หรือได้มีการแจ้งเตือนให้ดำเนินการแก้ไขอย่างเหมาะสมแล้วก่อนที่การละเมิดนั้นจะเกิดขึ้น[31]
คำขอใช้สิทธิของเจ้าของข้อมูล	คำขอใช้สิทธิของเจ้าของข้อมูลส่วนใหญ่เป็นการขอให้ลบข้อมูลส่วนบุคคล โดย DPO จะต้องพิจารณาว่าสถาบันการเงินมีความจำเป็นในการจัดเก็บข้อมูลนั้นต่อไปหรือไม่ หรือมีหน้าที่ต้องเก็บรักษาไว้ตามกฎหมายใดหรือไม่ นอกจากนี้ คำขอใช้สิทธิอาจมีความซับซ้อน (โปรดอ่านต่อใน “หัวข้อ 5.4 การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล”)

[31] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม (ตัวอย่างเช่น การส่งอีเมล์ผิดฝ่ายงานภายในองค์กร หรือการที่ลูกค้าเปิดเผยข้อมูลส่วนบุคคลให้ผู้อื่นทราบด้วยตนเองโดยมิได้ตั้งใจ ซึ่งสถาบันการเงินไม่มีส่วนเกี่ยวข้องกับการเปิดเผยข้อมูลนั้น)

เรื่องปลีกย่อยอื่นๆ	ตัวอย่างเช่น ฐานการประมวลผล ความจำเป็นในการจัดเก็บข้อมูล ศาสนาหรือกรุ๊ปเลือด การทำข้อมูลปลอม (Mock-up Data) การใช้ข้อมูลลูกค้าเพื่อทำโฆษณาเจาะจงเฉพาะรายบุคคล (Personalized Advertisement) การรักษาความมั่นคงปลอดภัยของข้อมูล การจัดทำแบบฟอร์มขอความยินยอม

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

(3) บันทึกการให้คำปรึกษาหารือ

เมื่อได้มีการปรึกษาหารือในประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลภายในสถาบันการเงิน DPO มีหน้าที่บันทึกผลการทบทวน ผลการประเมิน รวมไปถึงคำแนะนำต่างๆ ที่ให้ไว้กับทุกฝ่าย[32] หากผู้ควบคุมข้อมูลไม่เห็นด้วยกับคำแนะนำของ DPO ควรระบุเป็นลายลักษณ์อักษรไว้อย่างชัดเจนในเอกสาร พร้อมเหตุผลว่าเพราะเหตุใดผู้ควบคุมข้อมูลจึงเลือกที่จะไม่ปฏิบัติตามคำแนะนำของ DPO[33] นอกจากนี้ ในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล หลังจากได้มีการประเมินเหตุละเมิดข้อมูลส่วนบุคคลและเหตุนั้นสิ้นสุดลงแล้ว DPO และผู้ควบคุมข้อมูลควรร่วมกันเก็บบันทึกเหตุละเมิดข้อมูลส่วนบุคคล[34]

ผู้เขียนได้สอบถาม DPO และผู้ที่เกี่ยวข้องในสถาบันการเงินแต่ละแห่งว่ามีการจัดทำบันทึกข้อปรึกษาหารือหรือไม่ หากมีกรณีใดที่ต้องทำบันทึกดังกล่าวไว้บ้าง จากการสัมภาษณ์[35] พบว่า เนื่องจากกฎหมายยังไม่มีผลใช้บังคับจึงไม่ได้กำหนดขั้นตอนการบันทึกไว้อย่างชัดเจน ทำให้ในทางปฏิบัติสถาบันการเงินส่วนใหญ่ (12 แห่ง) ไม่ได้มีการจัดทำบันทึกข้อหารือกับ DPO หรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษรอย่างชัดเจน อย่างไรก็ตาม ได้จัดเก็บหลักฐานการให้คำปรึกษาและการตอบอยู่ในช่องทางต่างๆ ได้แก่ การสนทนาทางโทรศัพท์ อีเมล์ รายงานการประชุม หรือ Microsoft Teams Recording แล้วแต่กรณี เพื่อให้การให้คำปรึกษาหรือการแสดงความเห็นเป็นไปในทางเดียวกัน และเพื่อประโยชน์ในการจัดทำคำถามที่พบ

[32] Douwe Korff, and Marie Georges. Ibid, p.178.

[33] WP29, Guidelines on DPOs. Ibid, pp.13-14.

[34] Douwe Korff, and Marie Georges. Ibid, pp.215-216.

[35] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

บ่อย (Frequently asked questions - FAQ) ของแต่ละสถาบันการเงินต่อไป ในขณะที่สถาบันการเงินเฉพาะกิจขนาดเล็กแห่งหนึ่งกำหนดไว้ในคู่มือการทำงานว่าต้องบันทึกการปรึกษาหารือ หรือบันทึกรายงานการประชุมไว้ทุกครั้ง[36]

ตารางที่ 9 การจัดทำบันทึกข้อปรึกษาหารือของ DPO ผู้ให้สัมภาษณ์

การทำบันทึกข้อปรึกษาหารือกับ DPO	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
บันทึก[37]	-	-	1 แห่ง
ไม่ได้บันทึก[38]	5 แห่ง	2 แห่ง	5 แห่ง

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

สำหรับประเด็นการบันทึกข้อปรึกษาหารือกับ DPO ผู้เขียนมีความเห็นว่าควรมีการบันทึกการให้คำปรึกษาหารือและคำตอบจากทั้ง 2 ฝ่าย กล่าวคือ ฝ่ายผู้ขอคำปรึกษา และฝ่าย DPO หรือคณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นผู้ให้คำปรึกษา เพื่อประโยชน์ในการปฏิบัติงานของหน่วยธุรกิจ และเพื่อเป็นหลักฐานแสดงว่า DPO ได้ให้คำปรึกษาหรือคำแนะนำว่าอย่างไร อันจำเป็นหากหน่วยงานกำกับดูแลเข้ามาตรวจสอบการดำเนินงานของสถาบันการเงินและการดำเนินงานของ DPO เมื่อกฎหมายมีผลใช้บังคับแล้ว

3.1.2 การทบทวนการประมวลผลให้เป็นไปตามหลักการของกฎหมาย

DPO มีหน้าที่ทบทวนกระบวนการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินให้เป็นไปตามหลักการพื้นฐานของกฎหมาย เช่น หลักความโปร่งใสของการประมวลผลข้อมูล (Transparency) หลักการประมวลผลภายใต้วัตถุประสงค์ที่จำกัด (Purpose Limitation) หรือหลัก

[36] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[37] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม (คู่มือการทำงานของสถาบันการเงินกำหนดให้มีหน้าที่บันทึกข้อปรึกษาหารือ หรือรายงานการประชุมไว้ทุกครั้งที่มีการปรึกษาหรือให้คำแนะนำ)

[38] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม (เนื่องจากกฎหมายยังไม่มีผลใช้บังคับ ไม่มีการกำหนดขั้นตอนการบันทึกและไม่ได้บันทึกเป็นลายลักษณ์อักษรไว้อย่างชัดเจน โดยจัดเก็บหลักฐานการให้คำปรึกษาและการตอบคำถามอยู่ในช่องทางต่างๆ เช่น อีเมล์ รายงานการประชุม หรือ Online Recording)

ความจำเป็นในการประมวลผลข้อมูล (Data Minimization) เป็นต้น โดย DPO ควรใช้บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) เป็นพื้นฐานในการทบทวน ตั้งตำถาม และตอบคำถามในประเด็นต่างๆ โดยเฉพาะอย่างยิ่งในประเด็นดังต่อไปนี้[39]

1. สถานะของบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล (เช่น ใครเป็นผู้ควบคุมข้อมูล ใครเป็นผู้ควบคุมข้อมูลร่วม ใครเป็นผู้ประมวลผลข้อมูล หรืออื่นๆ ถ้ามี) หากไม่แน่ชัด ให้ตรวจสอบว่ามีข้อตกลงเกี่ยวกับการระบุสถานภาพของบุคคลที่ทำการประมวลผลข้อมูลหรือไม่
2. แผนกหรือฝ่ายงานใดภายในองค์กรเป็นผู้หน้าที่รับผิดชอบทางพฤตินัยในการประมวลผลข้อมูล และมีการระบุไว้อย่างเป็นทางการไว้ในเอกสารใดหรือไม่
3. มีการระบุวัตถุประสงค์ของการประมวลผลข้อมูลหรือไม่ อยู่ในเอกสารใด และมีขึ้นเพื่อวัตถุประสงค์เดียว หรือมากกว่า 1 วัตถุประสงค์ หากมีการประมวลผลเพื่อวัตถุประสงค์ที่มากกว่า 1 วัตถุประสงค์ องค์กรได้มีการระบุหรือไม่ว่าอะไรคือประสงค์หลัก และอะไรคือวัตถุประสงค์รอง รวมถึงวัตถุประสงค์รองนั้นเป็นไปตามวัตถุประสงค์หลักและมีความเกี่ยวข้องกันกับวัตถุประสงค์หลักหรือไม่[40]
4. วัตถุประสงค์หลักในการประมวลผลเป็นเหตุอันสมควรที่จะประมวลผล (fully justified) และเป็นไปโดยชอบธรรม (legitimate)

[39] Douwe Korff, and Marie Georges. Ibid, pp.172-178.

[40] หลักความเข้ากันได้ของวัตถุประสงค์ (Compatibility of purposes) ในปัจจุบันยังไม่มีการบัญญัติไว้ในกฎหมายไทย ในขณะที่ GDPR, Article 5(1)(b) กำหนดไว้อย่างชัดแจ้งว่าข้อมูลส่วนบุคคลจะถูกจัดเก็บเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง (specified) ชัดแจ้ง (explicit) และชอบด้วยกฎหมาย (legitimate) และไม่ถูกประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว โดย GDPR, Article 6(4)(a) – (e) มีเกณฑ์การพิจารณาว่าวัตถุประสงค์อย่างไรจะเป็นวัตถุประสงค์ที่เข้ากันได้ มีดังต่อไปนี้

1. ความเกี่ยวข้องระหว่างวัตถุประสงค์ใหม่กับวัตถุประสงค์เดิม
2. บริบทในการเก็บรวบรวมข้อมูล โดยเจ้าของข้อมูลน่าจะคาดหมายได้ตามสมควรถึงวัตถุประสงค์ใหม่
3. ลักษณะของข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น พิจารณาว่ามีข้อมูลอ่อนไหวเกี่ยวข้องด้วยหรือไม่
4. ผลกระทบต่างๆ ที่อาจเกิดขึ้นกับเจ้าของข้อมูลจากการประมวลผลตามวัตถุประสงค์ใหม่
5. มีการใช้มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลโดยเหมาะสมหรือไม่ เช่น การเข้ารหัส (encryption) หรือการทำข้อมูลแฝง (pseudonymization)

5. ข้อมูลที่ถูกประมวลผลนั้นเพียงพอ เกี่ยวข้อง และจำเป็นกับวัตถุประสงค์หลัก และมีมาตรการใดบ้างในการตรวจสอบว่าข้อมูลมีความเที่ยงตรงและเป็นปัจจุบัน รวมถึงมีมาตรการใดเพื่อที่จะแก้ไขและทำให้ข้อมูลเป็นปัจจุบัน หรือลบข้อมูลที่ไม่ถูกต้องหรือข้อมูลที่ไม่เป็นปัจจุบันออกไป มาตรการเหล่านี้เพียงพอหรือไม่ และมีทางเลือกอื่นหรือไม่ที่จะสามารถประมวลผลตามวัตถุประสงค์เดียวกัน โดยมีความเสี่ยงที่เกี่ยวข้องกับสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลที่น้อยกว่าวิธีเดิม
6. ข้อมูลส่วนบุคคลใดบ้างที่ถูกใช้หรือเปิดเผยสำหรับวัตถุประสงค์รอง รวมไปถึงวัตถุประสงค์ที่ไม่เกี่ยวข้อง และข้อมูลเหล่านี้เพียงพอ เกี่ยวข้องและจำเป็นสำหรับการประมวลผลในวัตถุประสงค์รอง วัตถุประสงค์ใหม่ และวัตถุประสงค์ที่ไม่เกี่ยวข้องหรือไม่[41]
7. วัตถุประสงค์รอง หรือ วัตถุประสงค์ใหม่ หรือวัตถุประสงค์ที่ไม่เกี่ยวข้องกับวัตถุประสงค์หลักในการประมวลผลนั้นเป็นเหตุอันสมควรที่จะประมวลผล และเป็นไปโดยชอบธรรม
8. ข้อมูลที่ถูกประมวลผลนั้นเพียงพอ เกี่ยวข้อง และจำเป็นกับวัตถุประสงค์รอง และมีมาตรการใดบ้างเพื่อตรวจสอบว่าข้อมูลนั้นเที่ยงตรงและเป็นปัจจุบัน รวมถึงมีมาตรการใดเพื่อที่จะแก้ไขและทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ หรือลบข้อมูลที่ไม่ถูกต้องหรือข้อมูลที่ไม่เป็นปัจจุบันออกไป มาตรการเหล่านั้นเพียงพอหรือไม่
9. ข้อมูลส่วนบุคคลนั้นได้มาเมื่อไหร่ อย่างไร จากใคร ในรูปแบบใด และแหล่งที่มาของข้อมูลเหล่านี้เหมาะสมหรือไม่ (เช่น ข้อมูลบางประเภทควรได้รับมาจากเจ้าของข้อมูลโดยตรงแทนการรับมาจากบุคคลที่สาม)
10. ฐานการประมวลผลข้อมูลส่วนบุคคล

[41] การประมวลผลข้อมูลตามวัตถุประสงค์ที่อยู่นอกเหนือขอบข่ายวัตถุประสงค์เดิมหรือวัตถุประสงค์หลักอาจส่งผลให้เกิดการประมวลผลที่เกินความจำเป็น อันขัดต่อหลักการประมวลผลภายใต้วัตถุประสงค์ที่จำกัด (Purpose Limitation) และหลักความจำเป็นในการประมวลผลข้อมูล (Data Minimization) ได้

11. ระยะเวลาของการจัดเก็บข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลอ่อนไหว มีความเหมาะสมหรือไม่ นอกจากนี้ มีวิธีการลบ ทำลาย หรือการทำให้ข้อมูลไม่สามารถระบุตัวตนได้อย่างไร วิธีการเหล่านั้นมีความเหมาะสมหรือไม่ สามารถเปลี่ยนเป็นการเก็บในรูปแบบ fully-anonymous ได้หรือไม่
12. เมื่อมีการทำข้อมูลนิรนาม จะทราบได้อย่างไรว่ามีการทำให้นิรนามจริง
13. เมื่อมีการลบหรือทำลายข้อมูล การลบหรือทำลายนั้นเป็นไปตามมาตรฐานภายในประเทศและระหว่างประเทศ
14. ข้อมูลเหล่านี้ถูกเปิดเผยไปยังบุคคลที่สามใดบ้าง ด้วยเหตุผลใด และข้อมูลเหล่านี้ถูกต้อง เกี่ยวข้อง เป็นปัจจุบัน และจำเป็นต่อวัตถุประสงค์ในการโอนให้บุคคลที่สามหรือไม่ และมีมาตรการเพื่อทำให้มั่นใจว่าข้อมูลนั้นถูกต้อง และเป็นปัจจุบันหรือไม่
15. เจ้าของข้อมูลนั้นได้รับแจ้งถึงประเด็นต่างๆที่ควรได้รับแจ้ง วิธีแจ้งและเวลาที่ได้รับแจ้งมีความเหมาะสมที่สุด และมีการแยกประเด็นระหว่างประเด็นที่จำเป็นและประเด็นทางเลือกอย่างชัดเจน
16. ข้อมูลที่ถูกส่งไปยังประเทศที่สามหรือองค์กรระหว่างประเทศนั้นเป็นไปตามมาตรการที่กฎหมายกำหนด หรือได้รับการยกเว้นใดบ้างหรือไม่[42]
17. หากมีการส่งข้อมูลไปยังประเทศที่สาม การส่งข้อมูลนี้เป็นไปตามคำสั่งของศาลหรือตามอำนาจรัฐของต่างประเทศหรือไม่ หากไม่มีข้อตกลงอย่างเป็นทางการ ผู้ควบคุมข้อมูลไม่มีความจำเป็นต้องส่งข้อมูล อย่างไรก็ตาม ในการตัดสินใจส่งข้อมูล ให้องค์กรขอรับคำปรึกษาจากผู้บริหารระดับสูง และ DPO ตลอดจนและอาจขอความเห็นเพิ่มเติมจากหน่วยงานกำกับดูแล
18. หากองค์กรต้องส่งข้อมูลไปยังประเทศที่สาม ต้องตรวจสอบนโยบายและรายละเอียดของมาตรการทางเทคนิคของประเทศปลายทาง เพื่อทำให้มั่นใจได้ว่าข้อมูลมีความปลอดภัยและเป็นความลับ[43]

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 และมาตรา 29 และ GDPR, Article 45, 46 และ 48

19. หากมีการใช้ระบบคลาวด์ (Cloud) ในการประมวลผลจะต้องตรวจสอบว่าคลาวด์ที่ใช้บริการนั้นได้รับการรับรอง[44]

20. DPO ควรทราบและเข้าใจถึงมาตรฐานที่เกี่ยวกับความปลอดภัยของข้อมูล[45]

หาก DPO พบว่าการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินนั้น ไม่ได้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ไม่ว่าจะในประเด็นใดก็ตาม DPO มีหน้าที่แจ้งให้บุคคลที่มีหน้าที่รับผิดชอบภายในองค์รับรู้ถึงข้อบกพร่องและเสนอแนะข้อแก้ไข และบางกรณีอาจต้องทำการระงับกิจกรรมการประมวลผลข้อมูลนั้น

สำหรับวิธีการศึกษาวิจัยนั้น ผู้เขียนได้ถามว่า “สถาบันการเงินของท่านมีขั้นตอนการทบทวนการปฏิบัติงานให้เป็นไปตามหลักการประมวลผลภายใต้วัตถุประสงค์ที่จำกัด (Purpose Limitation) และหลักความจำเป็นในการประมวลผลข้อมูล (Data Minimization) อย่างไร”

ผลการสัมภาษณ์[46] พบว่า สถาบันการเงินแต่ละแห่งได้มีการทบทวน ประเมินความถูกต้องและความจำเป็นในการจัดเก็บข้อมูลให้เป็นไปตามหลักกฎหมายเป็นประจำทุกปีหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ ขึ้นอยู่กับสถานการณ์การประมวลผลข้อมูลส่วนบุคคลในช่วงนั้นๆ โดยสถาบันการเงินแต่ละแห่งมีขั้นตอนที่แตกต่างกัน ดังนี้

ตารางที่ 10 วิธีการทบทวนการประมวลผลข้อมูลส่วนบุคคลของ DPO

วิธีทบทวนการประมวลผลข้อมูลของ DPO ในสถาบันการเงิน	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
ตรวจสอบตามกระบวนการรักษาความปลอดภัยสารสนเทศขององค์กรที่จัดขึ้น	5	2	6

[43] GDPR, Article 23

[44] DPO อาจพิจารณาจาก “Trusted Cloud – Data Protection Profile for Cloud Services (TCDP)”

[45] Douwe Korff, and Marie Georges. Ibid, p.177. (ในทางปฏิบัติ DPO ควรมีความรู้ความเข้าใจเกี่ยวกับมาตรฐานความปลอดภัยของข้อมูลเพิ่มเติม เพื่อให้สามารถทำหน้าที่ตรวจสอบการประมวลผลขององค์กรได้ เช่น ISO/IEC 27001:2013, 27002, 29100, 27018, 29134, 29151, 20889, 29184, JIS 15001:2006, BS 10012:2017, UNI Reference Practice) ซึ่งมีความสอดคล้องกับที่ ดร.สุนทรีย์ ส่งเสริม ได้ให้สัมภาษณ์ว่า “สถาบันการเงินอาจนำขั้นตอนตามกระบวนการของ ISO มาปรับใช้เพื่อให้มีการติดตามตรวจสอบการดำเนินการภายในองค์กรให้เป็นไปตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร”

[46] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

วิธีทบทวนการประมวลผลข้อมูลของ DPO ในสถาบันการเงิน	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
เป็นประจำทุกปี			
ตรวจสอบจาก ROPA	3	2	4
ให้ความเห็นต่อการประเมินความเสี่ยงของโครงการต่างๆ	1	-	1
นอกจากนี้ ปัจจุบันกระบวนการตรวจสอบความถูกต้องของการประมวลผลข้อมูลส่วนบุคคลโดย Internal Audit ของแต่ละสถาบันการเงินตามที่ ธปท. กำหนด ยังเป็นเพียงการตรวจสอบความพร้อมของการปฏิบัติตามกฎหมายเท่านั้น (PDPA Readiness) เนื่องจากการเลื่อนการบังคับใช้ของกฎหมาย			

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

สถาบันการเงินทั้งหมด 13 แห่ง (ขนาดใหญ่ 5 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 6 แห่ง) ที่ผู้เขียนได้ทำการสัมภาษณ์ นำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการคุ้มครองข้อมูล ได้แก่ การดูแลและจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลโดยให้สิทธิเฉพาะผู้ที่เกี่ยวข้องตามความจำเป็นที่จะเรียกดู ส่งต่อ แก้ไข หรือลบข้อมูลได้ รวมถึงจัดให้มีกระบวนการติดตามตรวจสอบระบบรักษาความปลอดภัยสารสนเทศตามกระบวนการของสถาบันการเงินที่มีอยู่แล้วเป็นประจำทุกปี โดยตรวจสอบส่วนที่เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เพิ่มเติม นอกจากนี้ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง กล่าวว่า “สถาบันการเงินได้จัดให้มีระบบอัพเดทข้อมูลส่วนบุคคลจากการทำธุรกรรมของลูกค้าโดยอัตโนมัติตามฐานสัญญาและฐานความยินยอมตลอดอายุของสัญญา หรือเมื่อลูกค้าถอนความยินยอม หรือเมื่อมีการผิดนัด หรือเมื่อมีการฟ้องร้อง”

สถาบันการเงิน 10 แห่ง (ขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 4 แห่ง) ตรวจสอบจาก ROPA เป็นหลัก จัดระเบียบ แก้ไขให้ข้อมูลมีความถูกต้องสมบูรณ์ และทำให้มั่นใจว่าได้จัดเก็บเฉพาะข้อมูลที่จำเป็น เช่น สถาบันการเงินหลายแห่งจะใช้คำถามว่ามีความจำเป็นต้องใช้สถานที่ประกอบพิธีหรือให้จัดอาหารประเภทใด แทนการเก็บข้อมูลศาสนาของพนักงาน

ทั้งนี้ สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่ง ได้ใช้ DPIA และกระบวนการจัดการของฝ่ายบริหารความเสี่ยงเป็นเครื่องมือการทบทวนประกอบกับวิธีการข้างต้น

นอกจากนี้ จากการสัมภาษณ์พบว่า[47] ฝ่ายตรวจสอบภายใน (Internal Audit) ของแต่ละสถาบันการเงินจะเข้ามาบทบาทหน้าที่ในการตรวจสอบความถูกต้องของการประมวลผลข้อมูลตามกระบวนการที่ธนาคารแห่งประเทศไทยกำหนด อย่างไรก็ดี เนื่องจากกฎหมายเลื่อนการบังคับใช้จึงทำให้การตรวจสอบของฝ่ายตรวจสอบภายของแต่ละสถาบันการเงินยังอยู่ในระดับเบื้องต้นเท่านั้น กล่าวคือ การตรวจสอบความพร้อมของการปฏิบัติตามกฎหมาย (PDPA Readiness)

อย่างไรก็ดี ในปัจจุบันยังไม่มีกฎหมายกำหนดเกี่ยวกับการจัดทำมาตรฐานการทบทวนการปฏิบัติงานให้เป็นไปตามกฎหมายอย่างชัดเจน ซึ่ง DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง[48] กล่าวว่า “มาตรฐานการทบทวนการปฏิบัติงานให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลขององค์กรอยู่ในระหว่างการรับฟังความคิดเห็นของหน่วยธุรกิจ และต้องการให้หน่วยงานกำกับดูแลหรือผู้ที่มีส่วนเกี่ยวข้องเร่งออกแนวปฏิบัติเรื่องดังกล่าวออกมาให้ชัดเจนโดยเร็ว”

3.1.3 การตรวจสอบประกาศแจ้งการประมวลผลข้อมูล (Privacy Notice) และแบบฟอร์มขอความยินยอม (Consent Form)

เอกสารที่มีความสำคัญมากที่สุดในการทบทวนและตรวจสอบ คือ ประกาศแจ้งการประมวลผลข้อมูล (Privacy notice)[49] (หรือในองค์กรบางแห่งอาจเรียกว่า “ประกาศเกี่ยวกับความเป็นส่วนตัว”) เนื่องจากสถาบันการเงินมีหน้าที่สร้างความเข้าใจแก่เจ้าของข้อมูลที่จะทำการเก็บรวบรวมและประมวลผลถึงรายละเอียดของกระบวนการดำเนินงาน ไม่ว่าจะเป็นการเก็บรวบรวม วัตถุประสงค์และวิธีการประมวลผล ฐานการประมวลผล การลบหรือทำลายข้อมูลส่วนบุคคล ชื่อบุคคลผู้ที่มีส่วนเกี่ยวข้อง รวมถึงมาตรการรักษาความปลอดภัยของข้อมูลที่องค์กรนำมาใช้ ไม่ว่าจะเป็นกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง[50] หรือกรณีเก็บข้อมูลมาจาก

---

[47] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[48] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[49] ในทางปฏิบัติองค์กรควรจัดให้มีนโยบายความเป็นส่วนตัว (Privacy Policy) ซึ่งเป็นภาพรวมแนวทางในการบริหารจัดการข้อมูลและคุ้มครองข้อมูลส่วนบุคคลขององค์กรโดยทั่วไปเพียงฉบับเดียว แล้วจึงลงรายละเอียดแต่ละโครงการหรือกิจกรรมลงในประกาศแจ้งการประมวลผลข้อมูล (Privacy Notice) เพื่อให้ง่ายต่อการแก้ไขรายละเอียดเฉพาะจุด และสะดวกต่อการแจ้งเจ้าของข้อมูลเมื่อมีการเปลี่ยนแปลงสาระสำคัญของการประมวลผล

[50] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23

แหล่งอื่น[51] ทั้งนี้เพื่อแสดงให้เห็นว่าองค์กรมีความโปร่งใสของการประมวลผลข้อมูล (Transparency) หากผู้ควบคุมข้อมูลไม่แจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ ต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท[52]

ก่อนหน้าที่จะกล่าวถึงองค์ประกอบของประกาศแจ้งการประมวลผล การนำเสนอประกาศแจ้งการประมวลผลเป็นสิ่งที่สำคัญไม่น้อยไปกว่าข้อความที่ต้องระบุในประกาศดังกล่าว กล่าวคือ ประกาศแจ้งการประมวลผลข้อมูลต้องชัดเจน[53] โปร่งใส อยู่ในรูปแบบบุคคลทั่วไปสามารถเข้าถึงได้ และใช้ภาษาที่บุคคลทั่วไปเข้าใจง่าย[54] โดยกำหนดหัวข้อใจตามความสำคัญของการประมวลผลให้ชัดเจนและง่ายต่อความเข้าใจ และแยกส่วนของรายละเอียดเพิ่มเติมออกเป็นอีกส่วนหนึ่งสำหรับเฉพาะเจ้าของข้อมูลที่สนใจอ่านรายละเอียดเพิ่มเติม (เช่น link หรือ pop-up message)

โดยสภาพประกาศแจ้งการประมวลผลข้อมูลเป็นข้อความอธิบายรายละเอียดของแต่ละกิจกรรมหรือโครงการใดๆ เกี่ยวกับการประมวลผลข้อมูลที่ทำขึ้นในช่วงเวลาใดช่วงเวลาหนึ่ง เมื่อสถาบันการเงินมีกิจกรรมหรือโครงการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลใหม่ๆ เกิดขึ้น DPO จึงควรเข้ามามีบทบาททบทวนและตรวจสอบประกาศแจ้งการประมวลผลเป็นประจำ โดยประกาศแจ้งการประมวลผลจะต้องประกอบด้วยรายละเอียด ดังตารางต่อไปนี้

---

[51] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25

[52] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 82

[53] หากเป็นประกาศแจ้งการประมวลผลของแอปพลิเคชันในโทรศัพท์หรืออุปกรณ์อิเล็กทรอนิกส์ขนาดพกพาอื่นๆ ควรใช้วิธีการนำเสนอข้อมูลแบบเป็นชั้น (layer) ควรกำหนดให้มีสัดส่วน และตำแหน่งของการวางข้อมูลให้เหมาะสมกับหน้าจอแสดงผลที่มีขนาดเล็กกว่าคอมพิวเตอร์

[54] หากประกาศแจ้งการประมวลผลมีส่วนที่เป็นการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ จะต้องใช้ความระมัดระวังป้องกันไม่ให้เกิดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์โดยไม่สมควร เช่น สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์หรือไม่ หรือแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม หรือกำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental mode) เพื่อป้องกันมิให้ผู้เยาว์ให้ข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์

ตารางที่ 11 องค์ประกอบของประกาศแจ้งการประมวลผลตามมาตรา 23 และมาตรา 25

รายละเอียดของการแจ้งการประมวลผล	กรณีได้รับข้อมูลจากเจ้าของข้อมูล[55]	กรณีได้รับข้อมูลจากแหล่งอื่น[56]
ชื่อและรายละเอียดการติดต่อขององค์กร	✓	✓
ชื่อและรายละเอียดการติดต่อของตัวแทนผู้รับผิดชอบ	✓	✓
ชื่อและรายละเอียดการติดต่อผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือ (ถ้ามี) และ DPO	✓	✓
วัตถุประสงค์ในการประมวลผลข้อมูล	✓	✓
ฐานการประมวลผลข้อมูล	✓	✓
ข้อมูลประเภทของข้อมูลส่วนบุคคลที่ได้รับมา	✓	✓
บุคคลที่สามที่เป็นผู้รับข้อมูล หรือประเภทของผู้รับข้อมูลส่วนบุคคล	✓	✓
รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ต่างประเทศ หรือองค์การระหว่างประเทศ (ถ้ามี)	✓	✓
ระยะเวลาในการเก็บข้อมูลส่วนบุคคล	✓	✓
สิทธิของเจ้าของข้อมูล	✓	✓
การแจ้งสิทธิยื่นคำร้องทุกข์ต่อหน่วยงานกำกับดูแล	✓	✓
แหล่งที่มาของข้อมูลส่วนบุคคล	✗	✓
รายละเอียดว่าเจ้าของข้อมูลมีหน้าที่ตามสัญญา หรือ ตามกฎหมายที่จะต้องให้ข้อมูลแก่ผู้ควบคุมข้อมูลหรือไม่ (ถ้ามี)	✓	✗
รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติ และโปรไฟลิ่ง (profiling) (ถ้ามี)	✓	✓
นโยบายความเป็นส่วนตัว (privacy policy) (ถ้ามี)	✓	✓

ที่มา: Thailand Data Protection Guidelines 3.0 - Version 3.0 Extension. หน้า.105

เอกสารอีกอย่างหนึ่งที่มีความสำคัญต่อการประมวลผลข้อมูลส่วนบุคคลซึ่ง DPO จะต้องทบทวนและตรวจสอบ โดยเฉพาะอย่างยิ่งสำหรับการประมวลผลข้อมูลในสถาบันการเงิน คือ แบบฟอร์มขอความยินยอม (Consent Form) เนื่องจากความยินยอมเป็นฐานการประมวลผลที่ทำให้

[55] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23

[56] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25

เจ้าของข้อมูลสามารถเลือกจัดการของข้อมูลของตนเองได้อย่างเต็มที่ที่สุด[57] หากองค์กรใช้ความยินยอมเป็นฐานการประมวลผล ก่อนดำเนินการประมวลผลข้อมูล จะต้องเชิญชวนให้เจ้าของข้อมูลยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆ[58] โดยที่เจ้าของข้อมูลอยู่ในสถานการณ์ที่สามารถเลือกที่จะปฏิเสธไม่ให้ความยินยอม และถ้าเจ้าของข้อมูลปฏิเสธ องค์กรก็ไม่อาจประมวลผลข้อมูลส่วนบุคคลได้ ด้วยเหตุนี้ หากสถาบันการเงินได้จัดทำประกาศแจ้งการประมวลผลข้อมูลอย่างเหมาะสม ย่อมเป็นการให้ข้อมูลสำคัญสำหรับการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลว่าจะให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนหรือไม่

การขอความยินยอมในการประมวลผลข้อมูลจากเจ้าของข้อมูลส่วนบุคคลไม่มีแบบฟอร์มมาตรฐานที่สามารถใช้ได้กับทุกกรณี กฎหมายเพียงแต่หลักการของความยินยอมไว้เท่านั้น[59] เนื่องจากขอบเขตและวัตถุประสงค์ที่จะขอความยินยอมนั้นจะแตกต่างกันออกไปตามแต่ละกรณี ซึ่งสามารถแยกพิจารณาองค์ประกอบความสมบูรณ์ของความยินยอม[60] ได้ดังต่อไปนี้

1. ความยินยอมที่ให้เกิดขึ้นจากความสมัครใจโดยอิสระ หากเจ้าของข้อมูลไม่สามารถเลือกได้อย่างแท้จริงว่าจะให้ความยินยอมหรือไม่ให้ความยินยอม เช่น ตกอยู่ในสถานการณ์บีบบังคับที่จะให้ความยินยอม (compelled to consent) หรือจะส่งผลเสียตามมาหากไม่ให้ความยินยอม[61] นอกจากนี้ ถ้าเจ้าของข้อมูล

---

[57] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guidlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 67-69. (อย่างไรก็ตาม เป็นที่ทราบกันดีว่าไม่ควรใช้ฐานความยินยอมในการประมวลผลข้อมูลอย่างพร่ำเพรื่อ เนื่องจากจะทำให้บุคคลเข้าใจผิดว่าสามารถถอนความยินยอมได้ทั้งที่ยังมีนิติสัมพันธ์กันอยู่ นอกจากนี้ การขอความยินยอมโดยไม่จำเป็นจะทำให้ลูกค้าหรือผู้ใช้บริการเกิดความสับสนและไม่ไว้วางใจการให้บริการ และอาจเกิดความเข้าใจผิดว่าองค์กรกำลังประมวลผลข้อมูลโดยไม่ชอบด้วยกฎหมายได้)

[58] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคหนึ่ง

[59] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19

[60] ผู้เขียนรวบรวมมาจาก Article 29 Data Protection Working Party (WP29), "Guidelines on consent under Regulation 2016/679," [Online] Accessed: 21 Jan 2021. Available from: https://ec.europa.eu/newsroom/article29/items/623051/en. pp.5-23.

[61] Article 29 Data Protection Working Party (WP29), "Opinion 15/2011 on the definition of consent," [Online] Accessed: 24 Oct 2021. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. p.12

ไม่สามารถปฏิเสธที่จะให้ความยินยอม หรือถอนความยินยอมไม่ได้เนื่องจากเกรงว่าจะได้รับผลกระทบมากเกินเหตุ ความยินยอมของเจ้าของข้อมูลในกรณีนี้จะเป็นความยินยอมที่ไม่สมบูรณ์[62] อีกทั้งการถอนความยินยอมจะต้องกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมตามสัญญาหรือตามกฎหมาย[63]

2. การขอความยินยอมต้องไม่อยู่ปะปนกับเงื่อนไขในการให้บริการหรือข้อความอื่น[64] และใช้ภาษาที่บุคคลทั่วไปเข้าใจได้ง่าย[65] เพื่อไม่ให้เกิดความเข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการ โดยเฉพาะอย่างยิ่งในกรณีที่การประมวลผลข้อมูลไม่จำเป็นสำหรับการให้บริการตามสัญญา
3. แจ้งวัตถุประสงค์ของการประมวลผลข้อมูลที่มีความเฉพาะเจาะจง (specific)[66] และไม่สามารถนำข้อมูลไปประมวลผลโดยใช้วัตถุประสงค์ใหม่ได้เองโดยปราศจากการขอความยินยอมใหม่ ซึ่งวัตถุประสงค์นั้นอาจมีเพียงวัตถุประสงค์เดียว หรือมีมากกว่า 1 วัตถุประสงค์ การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว ส่วนการใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลเลือกว่าจะให้ความยินยอมสำหรับวัตถุประสงค์ใด

[62] ผู้เขียนเรียบเรียงจาก GDPR, Recitals 42 และ 43 รวมถึง WP29. Opinion 15/2011 on the definition of consent. Ibid, p.12

[63] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคห้า

[64] ทั้งนี้ ในกรณีการขอความยินยอมในการเปิดเผยข้อมูลลูกค้าให้บุคคลอื่นเพื่อวัตถุประสงค์อื่นที่ไม่ใช่การตลาด (หมายถึง การเปิดเผยในกรณีที่หากลูกค้าไม่ให้ความยินยอมจะกระทบต่อการดำเนินการของผู้ให้บริการอย่างมีนัยสำคัญ หรือจะไม่สามารถให้บริการได้อย่างเป็นธรรมและต่อเนื่อง เช่น การเปิดเผยข้อมูลแก่ outsource เพื่อสนับสนุนการให้บริการของสถาบันการเงิน การเปิดเผยข้อมูลให้หน่วยงานราชการตามกฎหมาย หรือการเปิดเผยข้อมูลให้บริษัทพันธมิตรในลักษณะ co-brand) สถาบันการเงินสามารถกำหนดให้การเปิดเผยข้อมูลดังกล่าวเป็นส่วนหนึ่งของเงื่อนไขในการขอใช้บริการได้ โดยให้ระบุตัวอย่างวัตถุประสงค์ในการเปิดเผยข้อมูล ให้ลูกค้าทราบ เช่น เพื่อประโยชน์ในการดำเนินการติดตามทวงถามหนี้ โดยไม่จำเป็นต้องแจ้งชื่อบุคคลผู้รับข้อมูล

[65] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคสาม

[66] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคสาม และ GDPR, Article 6(1)(a)

4. เจ้าของข้อมูลได้รับข้อมูลเพียงพอก่อนตัดสินใจให้ความยินยอม (informed)[67] แต่เนื้อหาจะต้องมีความกระชับ ไม่ยาวจนเกินไป โดยการให้ข้อมูลอาจทำได้หลายรูปแบบ เช่น การเขียน ปากเปล่า วิดีโอ ข้อความเสียง ข้อความอิเล็กทรอนิกส์ pop-up screen หรือแชทบอท (chatbot)
5. ความยินยอมต้องชัดเจนไม่คลุมเครือ (unambiguous)[68] เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน ต้องไม่ใช่การขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเงียบเฉยหรือการเช็คถูกในช่องให้ประมวลผลข้อมูลไว้ก่อน (pre-ticked opt-in box) ไม่ถือเป็นความยินยอมที่ชัดเจน[69]

อนึ่ง ตามประกาศธนาคารแห่งประเทศไทยที่ สกส. 1/2561 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ได้กำหนดหลักเกณฑ์บางประการเกี่ยวกับแบบฟอร์มในการขอความยินยอมจากลูกค้าในกรณีที่สถาบันการเงิน (รวมถึงบริษัทที่ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงิน และ บริษัทที่ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงิน) ต้องการขอความยินยอมจากลูกค้าเพื่อวัตถุประสงค์ทางการตลาด ซึ่งผู้เขียนจะกล่าวต่อไปใน “หัวข้อ 5.5 แบบฟอร์มขอความยินยอม”

สำหรับการศึกษาวิจัยเพื่อให้ทราบว่าทางปฏิบัติ DPO ในแต่ละสถาบันการเงินมีส่วนร่วมในการทบทวนประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) และแบบฟอร์มขอความยินยอม (Consent Form) หรือไม่ และมีส่วนร่วมมากน้อยเพียงใด ผู้เขียนได้ใช้วิธีเก็บข้อมูลจากแบบสอบถาม รวมถึงการสัมภาษณ์บุคคลซึ่งอยู่ในคณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคลของ

---

[67] WP29, Guidelines on consent under Regulation 2016/679, Ibid, p.13. (WP29 มีความเห็นว่าผู้ควบคุมข้อมูลควรแจ้งให้เจ้าของข้อมูลทราบถึงประเด็นดังต่อไปนี้เป็นอย่างน้อยก่อนที่เจ้าของข้อมูลจะตัดสินใจให้ความยินยอม คือ ตัวตนของผู้ควบคุมข้อมูล วัตถุประสงค์ของการประมวลผลที่ต้องให้ความยินยอม ประเภทข้อมูลที่จะทำการเก็บรวบรวมและนำไปใช้ สิทธิของเจ้าของข้อมูลในการถอนความยินยอม ข้อมูลเกี่ยวกับการใช้ระบบอัตโนมัติในการประมวลผล (ถ้ามี) และความเสี่ยงของการโอนข้อมูลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลเพียงพอ)

[68] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคสอง และ GDPR, Article 4(11)

[69] WP29, Guidelines on consent under Regulation 2016/679, Ibid, p.16.

สถาบันการเงิน จำนวน 13 แห่ง พบว่า[70] ฝ่ายกฎหมายของสถาบันการเงินแต่ละแห่งจะเป็นผู้ร่างประกาศแจ้งการประมวลผลข้อมูลและแบบฟอร์มขอความยินยอม โดยผ่านการรับฟังความเห็นจากทุกหน่วยงานภายในองค์กร การร่างเอกสารดังกล่าวของแต่ละสถาบันการเงินจะให้ความสำคัญกับความโปร่งใส ใช้ภาษาที่บุคคลทั่วไปสามารถเข้าใจได้ง่าย[71] โดยปกติ DPO หรือคณะทำงานฯ ของสถาบันการเงินจะทำการทบทวนความถูกต้องสมบูรณ์และความเป็นปัจจุบันของประกาศแจ้งการประมวลผลและแบบฟอร์มขอความยินยอม อย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ซึ่งส่วนใหญ่การปรับปรุงเอกสารดังกล่าวแก้ไขไม่ได้เกิดขึ้นบ่อย และมักเป็นการเปลี่ยนแปลงรายละเอียดปลีกย่อยที่ยังคงไว้ซึ่งหลักการเดิม ตัวอย่างเช่น แก้ไขเพิ่มเติมชื่อหน่วยงานที่ต้องการเปิดเผยข้อมูล ปรับปรุงหรือยกเลิกรายละเอียดข้อมูลส่วนบุคคลที่จัดเก็บให้เหลือแต่เฉพาะข้อมูลที่จำเป็นต่อการประมวลผล ยกเลิกการเก็บข้อมูลศาสนาหรือข้อมูลกรุ๊ปเลือด

สำหรับจำนวนครั้งโดยเฉลี่ยที่ DPO ของแต่ละสถาบันการเงินทำการตรวจสอบหรือปรับปรุงประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคลและแบบฟอร์มขอความยินยอม ปรากฏตามตารางดังต่อไปนี้ (ทั้งนี้ ขณะทำการสัมภาษณ์ DPO ของสถาบันการเงินขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่งไม่สามารถระบุจำนวนครั้งที่ตนเคยตรวจสอบหรือปรับปรุงเอกสารดังกล่าวได้)

ตารางที่ 12 จำนวนครั้งโดยเฉลี่ยที่ DPO ตรวจสอบประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) และแบบฟอร์มขอความยินยอม (Consent Form)

การตรวจสอบของ DPO	**ขนาดใหญ่**	**ขนาดกลาง**	**ขนาดเล็ก**
ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice)	2-3 ครั้ง	2-3 ครั้ง	2-3 ครั้ง
แบบฟอร์มขอความยินยอม (Consent Form)	7-8 ครั้ง	2-3 ครั้ง	2-3 ครั้ง
หมายเหตุ: DPO ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดกลาง 1 แห่งยังไม่เคยมีส่วนร่วมในการตรวจสอบเอกสารข้างต้น เนื่องจากเอกสารดังกล่าวถูกจัดทำขึ้นก่อนมีการแต่งตั้ง ประกอบกับพ.ร.บ.ฯ ยังไม่มีผลใช้บังคับ และ			

[70] ผู้เขียนสรุปจาก บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[71] ผู้เขียนสรุปจาก บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ภายหลังยังไม่มีการเปลี่ยนแปลงอันมีนัยสำคัญ

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ผู้เขียนมีความเห็นว่าจำนวนครั้งของการตรวจสอบประกาศแจ้งการประมวลผลและแบบฟอร์มขอความยินยอม อาจไม่ได้ขึ้นอยู่กับขนาดของสถาบันการเงิน และไม่ใช่สิ่งบ่งชี้ที่แสดงถึงความเหมาะสมในการปฏิบัติหน้าที่ของ DPO หรือคณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร สถาบันการเงินควรกำหนดความถี่ของการตรวจสอบเอกสารดังกล่าวตามความเหมาะสม กล่าวคือ กำหนดกระบวนการทำงานให้ฝ่ายกฎหมายหรือฝ่ายงานที่เกี่ยวข้องปรึกษารายละเอียดการร่างเอกสารดังกล่าวกับ DPO ตั้งแต่ขั้นตอนแรกหรือกำหนดให้ฝ่ายงานต่างๆ ปรึกษาหารือกับ DPO เฉพาะกรณีที่มีการเปลี่ยนแปลงเนื้อหาอันเป็นสาระสำคัญของการประมวลผลข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลควรแจ้งต่อบุคคลที่จะถูกเก็บรวบรวมข้อมูล เช่น ชื่อผู้รับผิดชอบเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล วัตถุประสงค์ในการประมวลผล ฐานการประมวลผล สิทธิของเจ้าของข้อมูล ระยะเวลาการจัดเก็บ เป็นต้น ดังนั้น ถ้าผลิตภัณฑ์หรือการให้บริการใดของสถาบันการเงินไม่มีรายละเอียดของการประมวลผลอันเป็นสาระสำคัญเปลี่ยนแปลงไปจากที่กำหนดไว้ในประกาศแจ้งการประมวลผลและแบบฟอร์มขอความยินยอมฉบับเดิม การขอคำปรึกษาจาก DPO ในเรื่องดังกล่าวอีกย่อมทำให้การดำเนินงานเกิดความซ้ำซ้อนโดยปราศจากความจำเป็น

3.1.4 การมีส่วนร่วมกับคณะทำงาน หรือคณะกรรมการภายในองค์กรที่เกี่ยวข้อง

วิธีการหนึ่งที่ช่วยส่งเสริมให้ DPO ของสถาบันการเงินต่างๆ เข้ามามีส่วนร่วมในกระบวนการทำงานภายในองค์กร คือ DPO ควรเข้าร่วมประชุมกับกลุ่ม คณะทำงาน หรือคณะกรรมการบริหารโครงการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ทุกๆ ครั้งที่มีการตัดสินในที่มีผลกับการคุ้มครองข้อมูลส่วนบุคคล และจะต้องได้รับข้อมูลที่เกี่ยวกับการตัดสินใจในเวลาที่เหมาะสมเพื่อที่จะให้คำปรึกษาได้ นอกจากนี้ องค์กรจะต้องนำความเห็นของ DPO ไปพิจารณา หากมีข้อขัดแย้งกัน ให้จดบันทึกเหตุผลไว้เสมอว่าเหตุใดองค์กรจึงไม่ปฏิบัติตามคำแนะนำของ DPO[72]

[72] WP29 Guidelines on DPOs. Ibid, p.13.

ในการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การออกแบบและค่าเริ่มต้น (Data Protection by Design and by Default) สถาบันการเงินควรขอคำปรึกษากับ DPO ในขั้นตอนการวางแผนระบบเทคโนโลยีสารสนเทศที่ใช้รักษาความปลอดภัยของข้อมูลส่วนบุคคล ก่อนการนำมาใช้งานจริง[73] ซึ่ง DPO มีหน้าที่ให้ความช่วยเหลือฝ่ายงานเทคโนโลยีสารสนเทศ (IT) ในการระบุขอบเขตของการประมวลผลข้อมูลส่วนบุคคล เช่น ประเภทของข้อมูลที่จะจัดเก็บ วัตถุประสงค์ในการประมวลผล ฯลฯ รวมถึงประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลที่อาจเกิดขึ้น

ผู้เขียนได้สัมภาษณ์ DPO ของสถาบันการเงินต่างๆ จำนวน 13 แห่ง ว่ามีโอกาสได้ให้คำปรึกษาต่อคณะทำงานด้านข้อมูลส่วนบุคคล ผู้บริหาร หรือคณะกรรมการที่เกี่ยวข้องภายในองค์กรอย่างไรบ้าง และ DPO ของสถาบันการเงินแต่ละแห่งอยู่ในคณะกรรมการที่รับผิดชอบด้านการรักษาความปลอดภัยของข้อมูลหรือคณะกรรมการอื่นใดหรือไม่

ตารางที่ 13 จำนวน DPO ที่เป็นกรรมการภายในสถาบันการเงิน

สถานะ	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
DPO ที่เป็นกรรมการ	4 แห่ง	2 แห่ง	2 แห่ง
DPO ที่ไม่เป็นกรรมการ	1 แห่ง	-	4 แห่ง

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[74] DPO ของแต่ละสถาบันการเงินมีสถานะเป็น 'ที่ปรึกษา' และ 'ผู้สังเกตการณ์' ของสถาบันการเงิน ตลอดจนทำหน้าที่รายงานความคืบหน้า สถานะการปฏิบัติตามกฎหมายของสถาบันการเงิน และปัญหาที่เกิดขึ้นจากการดำเนินการให้เป็นไปตามกฎหมายต่อคณะกรรมการที่เกี่ยวข้องภายในสถาบันการเงิน โดย DPO ของสถาบันการเงิน 8 ท่าน เป็นหนึ่งในคณะกรรมการภายในสถาบันการเงิน ในขณะที่ DPO อีก 5 ท่านไม่ได้อยู่ในคณะกรรมการใดๆ

[73] EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.8

[74] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 14 คณะกรรมการภายภายในสถาบันการเงินที่ DPO ดำรงตำแหน่ง

คณะกรรมการภายในสถาบันการเงินที่ DPO ดำรงตำแหน่ง[75]	**ขนาดใหญ่ (ท่าน)**	**ขนาดกลาง (ท่าน)**	**ขนาดเล็ก (ท่าน)**
คณะกรรมการกำกับดูแลด้านความปลอดภัยเทคโนโลยีสารสนเทศ	3	2	1
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Committee)	3	1	1
คณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee)	2	-	1
คณะกรรมการบริหารความเสี่ยง (Risk Management Committee)	1	1	-
คณะกรรมการตรวจสอบ (Audit Committee)	-	1	-
คณะกรรมการสถาบันการเงิน (Board of Directors)	-	1	-

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ตามตารางข้างต้น คณะกรรมการภายในสถาบันการเงินที่ DPO ดำรงตำแหน่งนั้น จากการสัมภาษณ์พบว่า[76] ได้แก่ คณะกรรมการกำกับดูแลด้านความปลอดภัยสารสนเทศ (7 ท่าน) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Committee) (5 ท่าน) คณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) (3 ท่าน) คณะกรรมการบริหารความเสี่ยง (Risk Management Committee) (2 ท่าน) คณะกรรมการตรวจสอบ (Audit Committee) (1 ท่าน) และคณะกรรมการของสถาบันการเงิน (Board of Directors) (1 ท่าน)

[75] ตามตารางข้างต้น DPO จาก 8 แห่งซึ่งดำรงตำแหน่งเป็นกรรมการในคณะกรรมการภายในสถาบันการเงิน อาจเป็นกรรมการอยู่ในคณะกรรมการของสถาบันการเงินแห่งหนึ่งแห่งใดมากกว่า 1 คณะกรรมการ

[76] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

3.1.5 ความตระหนักรู้ถึงการมีอยู่และบทบาทหน้าที่ DPO ของคนในองค์กร

DPO จะต้องสามารถเข้าถึงข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่อย่างทันท่วงทีและให้คำปรึกษาได้อย่างเหมาะสม สถาบันการเงินควรกำหนดให้ DPO อยู่ในแผนผังองค์กรอย่างเป็นทางการ[77] อย่างไรก็ตาม กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย รวมถึงประกาศของธนาคารแห่งประเทศไทยไม่มีบัญญัติหน้าที่ให้สถาบันการเงินต่างๆ กำหนดให้ DPO อยู่ในแผนผังองค์กรอย่างชัดเจน

ผู้เขียนจึงได้สัมภาษณ์กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของแต่ละสถาบันการเงินว่าได้มีการกำหนดตำแหน่ง DPO ไว้ในแผนผังองค์กรอย่างเป็นทางการแล้วหรือไม่ หากยังไม่ได้กำหนด เพราะเหตุใด และบุคลากรภายในองค์กรทราบถึงการมีอยู่และหน้าที่ความรับผิดชอบของ DPO หรือไม่

ผลการสัมภาษณ์พบว่า[78] สถาบันการเงินแต่ละแห่งไม่ว่าจะเป็นสถาบันการเงินขนาดใหญ่ ขนาดกลาง หรือขนาดเล็ก ต่างมีความมั่นใจว่าบุคคลทุกระดับภายในองค์กรตั้งแต่คณะกรรมการผู้บริหารระดับสูง ไปจนถึงพนักงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ส่วนใหญ่ทราบถึงการมีอยู่และบทบาทหน้าที่ของ DPO เนื่องจากมีคำสั่งแต่งตั้ง DPO ของคณะกรรมการบริหารได้กำหนดอำนาจหน้าที่ไว้อย่างชัดเจน และมีการประกาศสื่อความให้พนักงานทราบถึงประเด็นดังกล่าวอย่างต่อเนื่อง

ตารางที่ 15 จำนวนสถาบันการเงินที่กำหนดตำแหน่ง DPO ในแผนผังองค์กร

	สถาบันการเงินที่กำหนดในแผนผังองค์กร (แห่ง)	สถาบันการเงินที่มิได้กำหนดในแผนผังองค์กร (แห่ง)
ขนาดใหญ่	3	2
ขนาดกลาง	1	1
ขนาดเล็ก	4	2

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

[77] EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.8

[78] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

โดยสถาบันการเงิน 8 แห่ง ได้กำหนดตำแหน่ง DPO ไว้ในแผนผังองค์กรอย่างเป็นทางการ ในขณะที่สถาบันการเงิน 5 แห่ง ไม่ได้กำหนดตำแหน่ง DPO ไว้ในแผนผังองค์กร โดยสถาบันการเงินที่ไม่ได้กำหนดให้ DPO อยู่ในแผนผังองค์กรมีเหตุผลดังต่อไปนี้[79]

- DPO ของธนาคารพาณิชย์ขนาดใหญ่ 2 แห่ง กล่าวว่า คำสั่งแต่งตั้งให้บุคคลภายในองค์กรเป็น DPO ได้กำหนดหน้าที่ความรับผิดชอบไว้อย่างชัดเจน โดยผู้บริหารและพนักงานทั่วไปทราบถึงการมีอยู่และหน้าที่ของ DPO แล้ว ประกอบกับบทบาทหน้าที่ของ DPO เป็นส่วนที่เพิ่มเติมจากขอบเขตงานเดิมของบุคคลที่เป็น DPO เท่านั้น จึงไม่มีความจำเป็นต้องกำหนดไว้ในแผนผัง
- ผู้ให้สัมภาษณ์จากธนาคารพาณิชย์ขนาดใหญ่แห่งหนึ่ง กล่าวว่า อยู่ในระหว่างการแต่งตั้ง DPO คนใหม่เนื่องจาก DPO คนเดิมได้ลาออก ทั้งนี้ ธนาคารได้กำหนดให้ DPO Office อยู่ในสังกัดของฝ่ายงานหนึ่งในองค์กรแล้ว ซึ่งประกอบด้วยบุคลากรจากหลากหลายหน่วยงาน เช่น ฝ่ายกฎหมาย ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ ฝ่ายบริหารความเสี่ยง หน่วยธุรกิจอื่น
- สถาบันการเงินขนาดกลางแห่งหนึ่ง มีการแต่งตั้ง DPO และจัดตั้งคณะทำงานขึ้น แต่ยังไม่มีการกำหนดโครงสร้างบริหารงานที่ชัดเจน เนื่องจากปัจจุบันกฎหมายไม่ได้กำหนดรายละเอียดในเรื่องดังกล่าว

3.1.6 ความสัมพันธ์ และอุปสรรคที่เกิดขึ้นจากการทำงานร่วมกับฝ่ายงานอื่นภายในองค์กร

เนื่องจากทางปฏิบัติ DPO ต้องมีความรู้ความเข้าใจบริบทขององค์กรและกระบวนการประมวลผลข้อมูลขององค์กรอย่างถ่องแท้ สามารถเข้าถึงข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ได้ การเข้าถึงนี้รวมถึงการติดต่อสัมพันธ์กับหน่วยงานต่างๆ ภายในองค์กรด้วย กล่าวคือ DPO ต้องประสานงานและทำงานร่วมกับผู้มีส่วนเกี่ยวข้อง (stakeholder) ทั้งหมดภายในองค์กร รวมถึงสามารถหาโอกาสในการติดต่อสื่อสารกับแผนกหรือฝ่ายงานต่างๆ เพื่อการปฏิบัติที่ตามกฎหมาย

[79] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

เป็นไปอย่างเหมาะสม[80] องค์กรควรจัดให้มีข้อมูลการติดต่อกับตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ในกฎ ระเบียบ มาตรฐานการปฏิบัติ คู่มือการทำงาน หรือเว็บไซต์ขององค์กรให้ชัดเจน

ประเด็นนี้อาจก่อให้เกิดปัญหาได้ในกรณีที่องค์กรแต่งตั้งบุคคลภายนอกเป็น DPO เช่น ตามสัญญารับจ้าง เป็นต้น เมื่อ DPO ซึ่งเป็นบุคคลภายนอกไม่ใช่ส่วนหนึ่งขององค์กรอาจส่งผลให้บุคคลดังกล่าวไม่เข้าใจวัฒนธรรมการทำงาน และกิจกรรมการประมวลผลข้อมูลขององค์กรที่ตนได้รับการแต่งตั้ง Commission nationale de l'informatique et des libertés (CNIL) ซึ่งเป็นหน่วยงานกำกับดูแลข้อมูลในประเทศฝรั่งเศสเห็นว่า DPO ควรเป็นบุคลากรภายในองค์กรของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่องค์กรขนาดกลางและขนาดเล็กโดยสภาพอาจไม่สามารถแต่งตั้งให้บุคคลภายในองค์กรเป็น DPO ได้[81]

อนึ่ง หากสถาบันการเงินแต่งตั้งบุคคลภายในองค์กรเป็น DPO ย่อมต้องใช้ความระมัดระวังมิให้เกิดการมีส่วนร่วมมากจนเกินไปอันจะส่งผลให้ DPO ขาดความเป็นอิสระในการตัดสินใจดำเนินงาน หรือเกิดความขัดแย้งทางผลประโยชน์ (Conflict of interest) ระหว่างบทบาทการทำงานต่อองค์กรกับหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล[82] ซึ่งผู้เขียนจะกล่าวถึงปัญหาที่เกี่ยวข้องกับเรื่องดังกล่าวต่อไปใน “หัวข้อ 3.4 ความขัดแย้งทางผลประโยชน์”

(1) ความสัมพันธ์ระหว่าง DPO กับหน่วยงานภายในสถาบันการเงิน

สำหรับการศึกษาวิจัยเพื่อให้ทราบว่า DPO ของสถาบันการเงินแต่ละแห่งในประเทศไทยมีความสัมพันธ์และต้องประสานงานกับแผนกหรือฝ่ายงานใดบ้าง ผู้เขียนจึงได้สอบถาม DPO รวมถึงคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินต่างๆ ว่านอกเหนือจากการรายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการของสถาบันการเงินนั้น ในทาง

---

[80] Douwe Korff, and Marie Georges. Ibid, p.134.

[81] CNIL, "Guide de Correspondant Informatique et Libertés," [Online] Accessed: 25 Oct 2021. Available from: https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf. p.6.

[82] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคท้าย

ปฏิบัติ DPO หรือคณะทำงานฯ มีความสัมพันธ์และการติดต่อสื่อสารกับหน่วยงานใดภายในองค์กรบ้าง โดยผู้ให้สัมภาษณ์สามารถตอบได้มากกว่า 1 หน่วยงาน

ตารางที่ 16 หน่วยงานภายในสถาบันการเงินที่ต้องทำงานร่วมกับ DPO

	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก	รวม
หน่วยงานที่มีความสัมพันธ์ร่วมกับ DPO เป็นประจำ				
หน่วยธุรกิจ (BU)	5	2	6	13
หน่วยงานที่มีความสัมพันธ์ร่วมกับ DPO เป็นครั้งคราว				
บริหารความเสี่ยง	5	2	6	13
ตรวจสอบภายใน	4	2	4	10
IT	3	2	3	8
กำกับการปฏิบัติตามกฎเกณฑ์	4	2	2	8
กฎหมาย	4	2	1	7
กำกับดูแลข้อมูล	1	-	1	2
จัดซื้อจัดจ้าง	1	-	-	1
ทรัพยากรบุคคล	-	-	1	1
สื่อสารองค์กร	-	-	1	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์[83] พบว่า DPO และคณะทำงานฯ ของสถาบันการเงินแต่ละแห่งมีความสัมพันธ์และการติดต่อสื่อสารกับทุกหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งกับหน่วยธุรกิจ (Business unit) บ่อยมากที่สุด โดยผ่านทางตัวแทนหรือผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นบุคลากรระดับผู้บริหารจากทุกสายงานขององค์กร (บุคคลดังกล่าวมีชื่อเรียกแตกต่างกันไปตามแต่ละสถาบันการเงิน เช่น PDPA Representative, DPO Champion หรือ Line-DPO เป็นต้น) บางสถาบันการเงินกำหนดให้มีตัวแทนดังกล่าวทำหน้าที่ประสานงานระหว่างหน่วยธุรกิจกับ DPO มากกว่า 1 คนต่อหนึ่งฝ่ายงาน DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเสริมว่า “องค์กรมีผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลประมาณ 200 ถึง 300 คน”

[83] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ขณะที่หน่วยงานอื่นอาจมีการติดต่อประสานงานกับ DPO บ้างเป็นครั้งคราวแต่ไม่มีลักษณะต้องทำงานร่วมกันเป็นประจำ ฝ่ายงานดังกล่าว เรียงลำดับตามหน่วยงานที่ทำงานร่วมกับ DPO เป็นครั้งคราวที่ผู้ให้สัมภาษณ์ตอบมากที่สุดไปยังน้อยที่สุด ได้แก่[84] ฝ่ายบริหารความเสี่ยง (13 แห่ง) ฝ่ายตรวจสอบภายใน (10 แห่ง) ฝ่ายเทคโนโลยีสารสนเทศ (IT) (8 แห่ง) ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) (8 แห่ง) ฝ่ายกฎหมาย (7 แห่ง) ฝ่ายกำกับดูแลข้อมูล (Data Governance) (2 แห่ง) ฝ่ายจัดซื้อจัดจ้าง (Procurement) (1 แห่ง) ฝ่ายทรัพยากรบุคคล (1 แห่ง) และฝ่ายสื่อสารองค์กร (1 แห่ง)

(2) ปัญหาที่เกิดขึ้นจากการทำงานร่วมกัน

นอกจากประเด็นความสัมพันธ์ระหว่างหน่วยงานภายในสถาบันการเงินกับ DPO ข้างต้น ผู้เขียนยังได้สัมภาษณ์เพิ่มเติมต่อไปว่า DPO และคณะทำงานฯ พบหรือคาดว่าจะพบปัญหาหรืออุปสรรคใดจากการทำงานร่วมกับหน่วยงานดังกล่าวบ้างหรือไม่ และเห็นว่าปัญหาหรืออุปสรรคนั้นเกิดจากสาเหตุใด หากมีปัญหาหรืออุปสรรคมากกว่า 1 อย่าง ให้เรียงลำดับความสำคัญของปัญหาหรืออุปสรรคเหล่านั้น โดยผลการสัมภาษณ์[85] พบว่าปัญหาที่เกิดขึ้นจากการทำงานร่วมกันระหว่าง DPO กับหน่วยงานต่างๆ ภายในสถาบันการเงินแต่ละแห่ง มีดังต่อไปนี้

ตารางที่ 17 ปัญหาที่เกิดขึ้นจากการทำงานร่วมระหว่าง DPO กับหน่วยงานภายในสถาบันการเงินที่ผู้ให้สัมภาษณ์กล่าวถึง

ปัญหาจากการทำงานร่วมกันที่ถูกกล่าวถึง	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
การตีความกฎหมาย	4	-	4
ความเข้าใจเรื่องการคุ้มครองข้อมูล	2	1	3
การปฏิบัติตามคำแนะนำ	1	1	3
ความเคร่งครัดของกฎหมาย	1	-	1
การพัฒนาระบบจัดการข้อมูลองค์กร	-	-	2

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

[84] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[85] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตามตารางข้างต้น ผู้ให้สัมภาษณ์ทำการประเมินอันดับความสำคัญหรือความจำเป็นเร่งด่วนของปัญหาดังกล่าวไว้ ดังต่อไปนี้

ตารางที่ 18 อันดับของปัญหาที่เกิดขึ้นจากการทำงานร่วมระหว่าง DPO กับหน่วยงานภายในสถาบันการเงินที่ผู้ให้สัมภาษณ์ทำการประเมิน

อันดับของปัญหา	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
1	ตีความกฎหมาย (3) ความเข้าใจ (1) ปฏิบัติตามคำแนะนำ (1)	ความเข้าใจ (1)	ตีความกฎหมาย (4) ความเข้าใจ (2)
2	ตีความกฎหมาย (1) ความเข้าใจ (1) ระบบจัดการข้อมูล (1)	ปฏิบัติตามคำแนะนำ (1)	ความเข้าใจ (1) ปฏิบัติตามคำแนะนำ (2) ความเคร่งครัดกฎหมาย (1)
3	ความเคร่งครัดกฎหมาย (1)		ปฏิบัติตามคำแนะนำ (1) ระบบจัดการข้อมูล (1)

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

(2.1) การตีความกฎหมาย

ปัญหาการตีความกฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นปัญหาที่ผู้ให้สัมภาษณ์ของสถาบันการเงิน 8 แห่งกล่าวถึง (สถาบันการเงินขนาดใหญ่ 4 แห่งและขนาดเล็ก 4 แห่ง) โดยสถาบันการเงินขนาดใหญ่ 3 แห่งและขนาดเล็ก 4 แห่งให้ความสำคัญเป็นอันดับแรก และสถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่สอง ด้วยเหตุนี้ผู้เขียนจึงจัดให้การตีความกฎหมายเป็นปัญหาที่มีสำคัญเป็น *‘อันดับแรก’*

จากการสัมภาษณ์พบว่า[86] ปัญหาดังกล่าวเกิดขึ้นจากสภาพกฎหมายในปัจจุบันที่ยังขาดความชัดเจนอย่างมาก เนื่องจากยังไม่มีการออกกฎหมายลำดับรองกำหนดรายละเอียดการดำเนินการตามหน้าที่ที่กฎหมายกำหนดในแต่ละเรื่อง ประกอบกับการเลื่อนการบังคับใช้ของกฎหมายออกไปเป็นวันที่ 1 มิถุนายน พ.ศ. 2565[87] การที่กฎหมายไม่มีความไม่ชัดเจนและไม่มีแนวปฏิบัติกลางของหน่วยงานกำกับดูแลส่งผลให้เกิดปัญหาการปรับปรุงนโยบายและระเบียบปฏิบัติของภาคธุรกิจสถาบันการเงินก็ตามมา ไม่ว่าจะเป็นบทบัญญัติเกี่ยวกับฐานการประมวลผลข้อมูลส่วนบุคคล เหตุละเมิดข้อมูลส่วนบุคคล หรือมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ต่างเป็นบทบัญญัติที่ล้วนสร้างภาระงานมหาศาลและทำให้เกิดความสับสนแก่สถาบันการเงินว่ามีหน้าที่และขอบเขตการปฏิบัติตามกฎหมายมากน้อยเพียงใด รวมถึงส่งผลกระทบต่อการลงทุนพัฒนาบุคลากรและระบบรักษาความปลอดภัยของข้อมูลให้เป็นไปตามมาตรฐานขั้นต่ำของกฎหมาย ปัจจุบันสถาบันการเงินแต่ละแห่งจึงต้องดำเนินการแก้ไขโดยยึดหลักการของ GDPR และแนวปฏิบัติที่เกี่ยวข้องไปชั่วคราว

(2.2) ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ปัญหาความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล[88] ซึ่งเป็นปัญหาที่ผู้ให้สัมภาษณ์ของสถาบันการเงิน 6 แห่งกล่าวถึง (สถาบันการเงินขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 3 แห่ง) โดยสถาบันการเงินขนาดใหญ่ 1 แห่ง ขนาดกลาง 1 แห่งและขนาดเล็ก 2

[86] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[87] หมายเหตุท้ายพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564 “เนื่องจากการปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่กฎหมายกำหนดนั้น มีรายละเอียดมากและซับซ้อน กับต้องใช้เทคโนโลยีขั้นสูงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพสมดังเจตนารมณ์ของกฎหมาย ประกอบกับสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ยังคงมีอยู่อย่างต่อเนื่องและรุนแรงยิ่งขึ้นจนถึงปัจจุบัน ส่งผลกระทบต่อเศรษฐกิจและสังคมโดยรวมเป็นอย่างมาก ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานและกิจการต่าง ๆ ทั้งภาครัฐและเอกชนจำนวนมากทั่วประเทศยังไม่พร้อมที่จะปฏิบัติตามพระราชบัญญัติดังกล่าว”

[88] ปัญหาความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในที่นี้ หมายถึง ความไม่ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลหรือความไม่เข้าใจหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย โดยเฉพาะอย่างยิ่งเป็นปัญหาที่เกิดจากหน่วยงานอื่นที่มิได้คลุกคลีกับการคุ้มครองข้อมูลเป็นประจำ เช่น หน่วยธุรกิจ (business unit)

แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง ด้วยเหตุนี้ผู้เขียนจึงจัดให้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของพนักงานเป็นปัญหาที่มีสำคัญเป็น *'อันดับที่สอง'*

จากการสัมภาษณ์พบว่า[89] ปัญหาข้างต้นเกิดขึ้นสืบเนื่องมาจากความไม่ชัดเจนของกฎหมาย เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เป็นกฎหมายที่มีลักษณะทางเทคนิคสูง จำเป็นต้องใช้เวลาและทรัพยากรจำนวนมากต่อการทำความเข้าใจและการปฏิบัติตาม นอกจากนี้ เจ้าหน้าที่อาวุโสฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง กล่าวว่า "ความไม่ชัดเจนของกฎหมายจะทำให้หน่วยงานภายในองค์กรเกิดความสับสนในเจตนารมณ์ของกฎหมายและท้ายที่สุดอาจส่งผลให้ไม่สามารถตามกฎหมายได้อย่างแท้จริง"

(2.3) การปฏิบัติตามคำแนะนำ

ปัญหาการปฏิบัติตามคำแนะนำของ DPO หรือคณะทำงานฯ ซึ่งเป็นปัญหาที่ผู้ให้สัมภาษณ์ของสถาบันการเงิน 5 แห่งกล่าวถึง (สถาบันการเงินขนาดใหญ่ 1 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 3 แห่ง) โดยสถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดกลาง 1 แห่งและขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม ด้วยเหตุนี้ผู้เขียนจึงจัดให้การปฏิบัติตามคำแนะนำของ DPO หรือคณะทำงานฯ เป็นปัญหาที่มีสำคัญเป็น *'อันดับที่สาม'*

จากการสัมภาษณ์พบว่า[90] DPO ของแต่ละสถาบันการเงินมีความเห็นไปได้ทิศทางเดียวว่า หน่วยธุรกิจขององค์กรเห็นว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เป็นกฎหมายที่เพิ่มภาระแก่การใช้ข้อมูล จึงไม่ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกับ DPO หรือคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

[89] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[90] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

(2.4) ความเคร่งครัดของการบังคับใช้กฎหมาย

ปัญหาความเคร่งครัดของการบังคับใช้กฎหมายซึ่งส่งผลกระทบต่อการดำเนินธุรกิจนี้ เป็นปัญหาที่ผู้ให้สัมภาษณ์ของสถาบันการเงิน 2 แห่งกล่าวถึง (สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่ง) โดยสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่สาม ด้วยเหตุนี้ผู้เขียนจึงจัดให้ปัญหาความเคร่งครัดในการบังคับใช้กฎหมายเป็นปัญหาที่มีสำคัญเป็น *'อันดับที่สี่'*

จากการสัมภาษณ์พบว่า[91] การมีระบบรักษาความปลอดภัยของข้อมูลหรือการปฏิบัติตามกฎหมายที่เข้มงวดมากเกินไปจนส่งผลเสียกับธุรกิจ อาจถึงขนาดที่อาจทำให้สถาบันการเงินแห่งนั้นสูญเสียฐานลูกค้าได้ ดังจะเห็นได้จากการที่ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งกล่าวว่า "การตีความกฎหมายฉบับนี้ไม่ควรมุ่งเน้นการคุ้มครองเจ้าของข้อมูลส่วนบุคคลมากเกินไป แต่จะต้องคำนึงถึงความได้สัดส่วนระหว่างการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและการนำข้อมูลส่วนบุคคลไปใช้ให้เกิดประโยชน์" ประเด็นดังกล่าวนี้ DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเสริมว่า "เมื่อเจ้าของข้อมูลโทรศัพท์มาขอความช่วยเหลือ เช่น บัตรเครดิตหาย หรือข้อมูลที่มีอยู่ไม่สามารถเบิกบัญชีได้ ฯลฯ สถาบันการเงินมีหน้าที่บันทึกเสียงโทรศัพท์ของลูกค้า แต่ในทางปฏิบัตินั้นการแจ้งรายละเอียดเกี่ยวกับการจัดเก็บข้อมูลส่วนบุคคลให้ครบถ้วนตามมาตรา 23 จะใช้เวลาสอบถามข้อมูลลูกค้านานเกินไปและอาจทำให้สูญเสียฐานลูกค้าได้ จึงควรมีกฎหมายกำหนดข้อยกเว้นในกรณีนี้"

(2.5) การพัฒนาระบบบริหารจัดการข้อมูลของสถาบันการเงิน

ปัญหาการพัฒนาระบบบริหารจัดการข้อมูลของสถาบันการเงินเป็นปัญหาที่ผู้ให้สัมภาษณ์ของสถาบันการเงิน 2 แห่งกล่าวถึง (สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่ง) โดยสถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม ด้วยเหตุนี้ผู้เขียนจึงจัดให้การพัฒนาระบบบริหารจัดการข้อมูล

[91] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ของสถาบันการเงินเป็นปัญหาที่มีสำคัญเป็น *'อันดับที่สี่' ร่วมกับปัญหาความเคร่งครัดในการบังคับใช้กฎหมายในข้อก่อนหน้านี้*

จากการสัมภาษณ์พบว่า[92] DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า "เกิดจากระบบที่มีความซับซ้อนและข้อจำกัดด้านเทคโนโลยีของสถาบันการเงิน" ส่วน DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งชี้ว่า "เกิดจากระบบจัดการและรักษาความปลอดภัยของข้อมูลถูกจัดทำโดยบริษัทแม่ที่อยู่ที่ต่างประเทศ"

3.2 ทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย

โดยหลักผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่สนับสนุนการปฏิบัติหน้าที่ของ DPO โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่[93] ตลอดจนได้รับการฝึกอบรมเพื่อธำรงไว้ซึ่งความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูล[94] โดยทรัพยากรดังกล่าว อาจรวมถึง[95]

- การให้เวลาเพียงพอในการทำงานของ DPO[96]
- การสนับสนุนในลักษณะของงบประมาณที่ใช้ดำเนินกิจกรรม โครงสร้างพื้นฐาน และพนักงานสนับสนุน
- การสื่อสารองค์กรเกี่ยวกับการแต่งตั้งและบทบาทหน้าที่ของ DPO

---

[92] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[93] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคสอง

[94] GDPR, Article 38(2)

[95] WP29, Guidelines on DPOs. Ibid, p.14

[96] DPEXNetwork, "Issues and Challenges faced by Data Protection Officers in Singapore (Part I)," [Online] Accessed: 28 Jan 2564. Available from: https://www.dpexnetwork.org/articles/issues-and-challenges-faced-data-protection-officers-singapore-part-i/ (จากผลสำรวจในประเทศสิงคโปร์เรื่องประเด็นปัญหาและความท้าทายของ DPO เมื่อวันที่ 8 มิถุนายน 2563 พบว่าเนื่องจาก DPO ขององค์กรต่างๆ ในประเทศสิงคโปร์เป็นจำนวนไม่น้อยกว่า 88% ต้องปฏิบัติหน้าที่ที่มีต่อองค์กรควบคู่ไปกับการเป็น DPO (Double-hatting) ทำให้มีชั่วโมงการทำงานคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอ โดยประมาณ 63% ใช้เวลาปฏิบัติหน้าที่ของ DPO น้อยกว่าหนึ่งในสี่ของชั่วโมงการทำงานทั้งหมด)

- การเข้าถึงบริการอื่น ๆ ขององค์กรเพื่อสนับสนุนการปฏิบัติหน้าที่ของ DPO (เช่น การบริหารจากฝ่ายทรัพยากรบุคคล ฝ่ายกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายรักษาความปลอดภัยของข้อมูล ฯลฯ)
- การฝึกอบรมอย่างต่อเนื่อง

ทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ของ DPO ขึ้นอยู่กับขนาดขององค์กรและลักษณะการดำเนินกิจการ ยิ่งองค์กรมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความซับซ้อนหรือข้อมูลที่ทำการประมวลผลเป็นข้อมูลอ่อนไหวมากเพียงใด ทรัพยากรที่ผู้ควบคุมหรือผู้ประมวลผลจัดหาจะมีมากเกินตามลำดับ จึงจะทำให้การคุ้มครองข้อมูลส่วนบุคคลสามารถประสบผลสำเร็จในทางปฏิบัติได้ (นอกจากนี้การได้รับทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ DPO ยังส่งผลโดยตรงต่อความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO อีกด้วย ซึ่งผู้เขียนจะกล่าวต่อไปใน “หัวข้อ 3.3 ความเป็นอิสระ”) และหาก DPO ต้องการทรัพยากรใดเพิ่มเติมจำเป็นต้องได้รับการอนุมัติจากผู้บริหารองค์กร

สำหรับวิธีการศึกษาวิจัย ผู้เขียนได้เก็บข้อมูลจากการตอบแบบสอบถามของ DPO และผู้ปฏิบัติงานในคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน 13 แห่งเกี่ยวกับทรัพยากรที่ผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลต้องการจากองค์กร โดยแบ่งทรัพยากรที่บุคคลดังกล่าวอาจต้องการออกเป็น บุคลากร เครื่องมือและเทคโนโลยี การเข้ารับการฝึกอบรม งบประมาณและค่าใช้จ่าย การเข้าถึงข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย การจ้างที่ปรึกษาซึ่งเป็นบุคคลภายนอก และการประสานงานกับหน่วยงานกำกับดูแล หรืออื่นๆ (ถ้ามี) โดยผู้ตอบแบบสอบถามสามารถเลือกทรัพยากรที่ต้องการได้มากกว่า 1 ทรัพยากร กรณีที่ผู้ตอบเลือกมากกว่า 1 ทรัพยากร ผู้เขียนได้ทำสัมภาษณ์เพิ่มเติมว่าบุคคลดังกล่าวมีความต้องการทรัพยากรใดมากที่สุด และทรัพยากรใดที่ต้องการน้อยที่สุด ตามลำดับ และมีปัญหาเกี่ยวกับทรัพยากรในด้านใดเกิดขึ้นหรือไม่

ผลการสำรวจพบว่า ทรัพยากรที่ DPO และผู้ปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินแต่ละแห่งกล่าวถึง มีดังต่อไปนี้[97]

[97] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 19 ปัญหาทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ที่ DPO ผู้ให้สัมภาษณ์กล่าวถึง

ปัญหาด้านทรัพยากรที่ถูกกล่าวถึง	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
บุคลากร	5	2	5
เครื่องมือและเทคโนโลยี	4	1	5
การฝึกอบรมความรู้	2	1	5
งบประมาณ	2	1	4
การเข้าถึงข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย	2	1	3
การจ้างที่ปรึกษาซึ่งเป็นบุคคลภายนอก	3	0	3
การประสานงานกับหน่วยงานกำกับดูแล	2	0	3

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ตามตารางข้างต้น DPO ผู้ให้สัมภาษณ์ทำการประเมินอันดับความสำคัญของทรัพยากรแต่ละด้าน ตามอันดับที่ปรากฏดังต่อไปนี้

ตารางที่ 20 อันดับของทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ DPO ที่ผู้ให้สัมภาษณ์ทำการประเมิน

อันดับของทรัพยากร	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
1	บุคลากร (3) จ้างที่ปรึกษา (1) หน่วยงานกำกับดูแล (1)	เครื่องมือ-เทคโนโลยี (1) เข้าถึงข้อมูลที่จำเป็น (1)	บุคลากร (5)
2	บุคลากร (1) เครื่องมือ-เทคโนโลยี (2) จ้างที่ปรึกษา (1)	บุคลากร (1) งบประมาณ (1)	เครื่องมือ-เทคโนโลยี (1) การฝึกอบรมความรู้ (1) งบประมาณ (3) จ้างที่ปรึกษา (1)
3	บุคลากร (1) เครื่องมือ-เทคโนโลยี (1) หน่วยงานกำกับดูแล (1)	บุคลากร (1) การฝึกอบรมความรู้ (1)	เครื่องมือ-เทคโนโลยี (1) การฝึกอบรมความรู้ (3) งบประมาณ (1) เข้าถึงข้อมูลที่จำเป็น (1)
4	การฝึกอบรมความรู้ (2)	-	เครื่องมือ-เทคโนโลยี (1) เข้าถึงข้อมูลที่จำเป็น (2)

			จ้างที่ปรึกษา (1) หน่วยงานกำกับดูแล (1)
5	เครื่องมือ-เทคโนโลยี (1) งบประมาณ (1) เข้าถึงข้อมูลที่จำเป็น (2)	-	เครื่องมือ-เทคโนโลยี (2) การฝึกอบรมความรู้ (1) หน่วยงานกำกับดูแล (1)
6	จ้างที่ปรึกษา (1)	-	หน่วยงานกำกับดูแล (1)
7	งบประมาณ (1)	-	จ้างที่ปรึกษา (1)

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

3.2.1 บุคลากร

บุคลากรในที่นี้ หมายถึง พนักงานภายในสถาบันการเงินที่สามารถใช้เวลาทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลกับ DPO หรือคณะทำงานฯ แต่ไม่รวมถึงพนักงานจากหน่วยงานหรือฝ่ายงานอื่นภายในองค์กรที่ให้ความช่วยเหลือเป็นครั้งคราว

จากแบบสอบถามพบว่า[98] บุคลากรเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 12 แห่ง (ขนาดใหญ่ 5 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 5 แห่ง) ซึ่งสถาบันการเงินขนาดใหญ่ 3 แห่งและขนาดเล็ก 5 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่สาม ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้บุคลากรเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการมากที่สุดเป็น *‘อันดับแรก’*

จากการสัมภาษณ์พบว่า[99] DPO ของสถาบันการเงินส่วนใหญ่ (9 แห่ง) ชี้ถึงปัญหาด้านบุคลากรไปในทำนองเดียวกันว่า “พนักงานของแต่ละสถาบันการเงินต่างมีความรับผิดชอบงานไม่ต่ำกว่า 2 เรื่อง จึงต้องการบุคลากรที่สามารถทำงานเต็มเวลา (full-time) หรือต้องการเพิ่มจำนวนพนักงานเพื่อให้สามารถขับเคลื่อนงานคุ้มครองข้อมูลส่วนบุคคลได้เร็วยิ่งขึ้น แต่ปัจจุบันติดมติของคณะกรรมการผู้บริหารจึงยังไม่สามารถทำได้ เนื่องจากการเลื่อนการบังคับใช้ของกฎหมายและความร้ายแรงของสถานการณ์โรคระบาด Covid-19 จึงทำให้สถาบันการเงินต่างๆ ต้องทุ่มเทกำลังคนให้กับ

[98] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[99] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

งานด้านอื่นที่ไม่ใช่งานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” นอกจากนี้ DPO ของสถาบันการเงินเฉพาะกิจ 2 แห่ง กล่าวว่า “ประสบปัญหาที่ไม่สามารถเพิ่มพนักงานเพื่อมาทำงานคุ้มครองข้อมูลส่วนบุคคลเนื่องจากองค์กรมีสภาพเป็นรัฐวิสาหกิจ มีขั้นตอนการปรับเปลี่ยนโครงสร้างที่ขาดความยืดหยุ่น เพราะต้องขออนุญาตกระทรวงการคลัง และถึงแม้ว่าจะมีข้อยกเว้นกรณีจัดตั้งฝ่ายงานใหม่ภายใต้หน่วยงานเดิมที่ทำให้ไม่ต้องขออนุญาต กรณีดังกล่าวผู้ให้สัมภาษณ์ก็มีความกังวลว่าอาจเกิดปัญหาความเป็นอิสระตามมา”

ในประเด็นปัญหาข้างต้น ผู้เขียนมีความเห็นว่าปัญหาเรื่องกำลังคนไม่เพียงพอต่อการทำงานด้านคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินเป็นปัญหาที่เกิดขึ้นในสถาบันการเงินทั้งภาคเอกชนและภาครัฐ ซึ่งผู้ปฏิบัติงานต้องแสดงให้คณะกรรมการผู้บริหารขององค์กรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Tone from the Top) รวมถึงผลที่ตามมาหากองค์กรเลือกที่จะไม่ปฏิบัติตามหรือไม่สามารถปฏิบัติตามมาตรฐานที่กฎหมายกำหนดอย่างเพียงพอ ทั้งนี้ทางเลือกที่เป็นไปได้นอกเหนือจากการเพิ่มจำนวนบุคลากรอาจเป็นการให้เวลาทำงานแก่งานคุ้มครองข้อมูลส่วนบุคคลมากขึ้น ส่วนประเด็นปัญหาความเป็นอิสระในกรณีที่ตั้งฝ่ายงานคุ้มครองข้อมูลส่วนบุคคลขึ้นภายในหน่วยงานที่มีอยู่เดิม ผู้เขียนได้อภิปรายไว้ใน “หัวข้อที่ 3.3 ความเป็นอิสระ”

อีกประการหนึ่ง DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเสริมว่า[100] “ในอนาคตเมื่อกฎหมายมีผลใช้บังคับ มีความจำเป็นต้องมีบุคลากรที่มีความรู้มาช่วยงาน องค์กรไม่สามารถพึ่งพาการใช้ระบบแต่เพียงอย่างเดียวได้” สำหรับประเด็นความรู้ความเข้าใจของผู้ปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคล ผู้เขียนมีความเห็นว่าต้องเป็นผู้มีความรู้ความเข้าใจอย่างใดอย่างหนึ่งดังต่อไปนี้เป็นอย่างน้อย คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล การดำเนินธุรกิจขององค์กร การควบคุมกระบวนการทำงาน การบริหารจัดการความเสี่ยง หรือเทคโนโลยีสารสนเทศ โดยขึ้นกับภูมิหลัง (background) และความเชี่ยวชาญของ DPO และบุคลากรในคณะทำงานฯ ว่าต้องการบุคลากรด้านใดที่ขาดไปเพิ่มเติม (สามารถอ่านรายละเอียดเพิ่มเติมใน “หัวข้อ 4.2 ความต้องการเพิ่มพูนความรู้ความเข้าใจ”)

[100] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

3.2.2 เครื่องมือและเทคโนโลยี

เครื่องมือและเทคโนโลยีในที่นี้ คือ อุปกรณ์ ซอฟต์แวร์ หรือสิ่งอำนวยความสะดวกอย่างอื่นที่ช่วยในการกำกับการประมวลผลของสถาบันการเงินเป็นไปตามกฎหมาย (PDPA Compliance tool) แต่ละเรื่อง เช่น ซอฟต์แวร์บันทึกรายการกิจกรรมการประมวลผล ซอฟต์แวร์บันทึกและตรวจสอบเหตุรั่วไหลของข้อมูลรวมถึงเหตุการณ์อื่นที่กระทบต่อข้อมูลส่วนบุคคล เครื่องมือประเมินผลกระทบของการคุ้มครองข้อมูลส่วนบุคคล (DPIA) หรือเครื่องมือติดตามการประมวลผลของบุคคลที่สาม

จากแบบสอบถามพบว่า[101] เครื่องมือและเทคโนโลยีเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 10 แห่ง (ขนาดใหญ่ 4 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 5 แห่ง) ซึ่งสถาบันการเงินขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 2 แห่งและขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ผู้เขียนจึงจัดอันดับให้เครื่องมือและเทคโนโลยีเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการมากเป็น *‘อันดับสอง’*

สำหรับผลการสัมภาษณ์[102] DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวถึงสาเหตุที่ต้องการเครื่องมือและเทคโนโลยีเพิ่มเติมว่า “เนื่องจากความไม่ชัดเจนของกฎหมายทำให้แต่ละสถาบันการเงินเกิดความกังวลเกี่ยวกับความคุ้มค่าในการลงทุนพัฒนาระบบบริหารจัดการข้อมูล” DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งเสริมว่า “ซอฟต์แวร์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในท้องตลาดปัจจุบันมีราคาแพง หรือไม่สามารถรองรับ ROPA ตามมาตรา 39 ได้ทั้งหมด” นอกจากนี้ DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “องค์กรมีระบบจัดการข้อมูลที่มีความซับซ้อนและมีข้อจำกัดด้านเทคโนโลยี” และสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งมีระบบรักษาความปลอดภัยของข้อมูลถูกจัดทำโดยบริษัทแม่ที่อยู่ในต่างประเทศ

ประเด็นเรื่องความคุ้มค่าในการลงทุนพัฒนาระบบจัดการข้อมูลส่วนบุคคล ผู้เขียนเห็นว่าภายหลังจากที่มีกฎหมายลำดับรองกำหนดหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

[101] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[102] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตลอดจนเมื่อมีการกำหนดขอบเขตและมาตรฐานขั้นต่ำของหน้าที่ดำเนินงานคุ้มครองข้อมูลส่วนบุคคลในแต่ละเรื่องจนครบถ้วน ปัญหาเหล่านี้น่าจะหมดไป โดยในระหว่างที่ยังไม่มีการออกกฎหมายกำหนดรายละเอียดในเรื่องดังกล่าวไว้ แต่ละสถาบันการเงินควรแลกเปลี่ยนความรู้ความเข้าใจเรื่องวิธีการดำเนินงานและร่วมกันพัฒนาแนวปฏิบัติต่างๆ มาใช้ตามความเหมาะสมไปพลางก่อน

3.2.3 การฝึกอบรมความรู้

การฝึกอบรมความรู้ในที่นี้ หมายถึง การเข้ารับการฝึกอบรมความรู้และแนวทางในการดำเนินงานด้านคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรทุกระดับภายในสถาบันการเงิน ตั้งแต่ระดับผู้บริหาร ระดับผู้ปฏิบัติงานโดยตรง และระดับพนักงานทั่วไป ไม่ว่าจะเป็นการเข้าร่วมประชุมสัมมนา การอบรมออนไลน์ การทำเวิร์คช็อป (Workshop) หรือการฝึกอบรมรูปแบบอื่นๆ ทั้งที่สถาบันการเงินจัดขึ้นเองหรือการจัดฝึกอบรมโดยหน่วยงานภายนอกที่อนุญาตให้ผู้ปฏิบัติงานเข้าร่วม

จากแบบสอบถามพบว่า[103] การฝึกอบรมความรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 8 แห่ง (ขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 5 แห่ง) ซึ่งสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดกลาง 1 แห่งและขนาดเล็ก 3 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดใหญ่ 2 แห่งให้ความสำคัญเป็นอันดับที่สี่ และสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้การฝึกอบรมความรู้เป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการมากเป็น *‘อันดับสาม’*

สำหรับรายละเอียดเกี่ยวกับการฝึกอบรมความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลภายในสถาบันการเงิน ผู้เขียนจะกล่าวถึงและอภิปรายต่อไปใน “หัวข้อ 4.5 การจัดฝึกอบรมความรู้ภายในสถาบันการเงิน”

[103] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

3.2.4 งบประมาณ

งบประมาณในที่นี้ คือ งบประมาณที่สถาบันการเงินจัดสรรไว้สำหรับงานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอต่อการปฏิบัติหน้าที่ตามกฎหมาย รวมถึงค่าใช้จ่ายที่จำเป็นต่างๆ ที่ผู้ปฏิบัติงานสามารถเบิกได้

จากแบบสอบถามพบว่า[104] งบประมาณเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 7 แห่ง (ขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 4 แห่ง) ซึ่งสถาบันการเงินขนาดกลาง 1 แห่งและขนาดเล็ก 3 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า และสถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่เจ็ด ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้งบประมาณเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการเป็น *‘อันดับสี่’*

จากการสัมภาษณ์[105] ผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “หน่วยงานภายในสถาบันการเงินต่างมุ่งเน้นเกี่ยวกับธุรกิจดิจิทัลที่สร้างรายได้ให้แก่องค์กรมากกว่าการลงทุนดำเนินการให้เป็นไปตามกฎหมายหรือค่าใช้จ่ายจำนวนมากในการให้ได้มาซึ่งใบรับรองคุณวุฒิของผู้ประกอบวิชาชีพคุ้มครองข้อมูล” นอกจากนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินต่างๆ ไม่ว่าขนาดใหญ่ ขนาดกลาง หรือขนาดเล็กยังกล่าวถึงปัญหานี้ไปในทางเดียวกันว่า เนื่องจากความไม่ชัดเจนของข้อกฎหมายและกฎระเบียบที่กำลังจะออก สถาบันการเงินจึงไม่ทราบว่าต้องจัดสรรงบประมาณและค่าใช้จ่าย บุคลากร เครื่องมือและเทคโนโลยีมากน้อยเพียงใดจึงจะเป็นไปตามมาตรฐานขั้นต่ำของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่สามารถประเมินความคุ้มค่าเมื่อเปรียบเทียบกับความเสี่ยงที่สถาบันการเงินจะถูกปรับในกรณีที่เกิดการรั่วไหลของข้อมูล”

ประเด็นเรื่องการจัดสรรงบประมาณ ผู้เขียนเห็นว่าในระหว่างที่ยังไม่มีการออกกฎหมายกำหนดรายละเอียดในเรื่องหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล การจัดการสิทธิของเจ้าของข้อมูล รวมถึงมาตรฐานขั้นต่ำในการปฏิบัติหน้าที่ในแต่ละเรื่อง ควรมีการจัดทำแนวปฏิบัติต่างร่วมกันของภาคสถาบันการเงินมาใช้ตามความเหมาะสมไปก่อน โดย DPO รวมทั้งผู้บริหารจากฝ่ายงานที่เกี่ยวข้องควรปรึกษาหารือองบประมาณและค่าใช้จ่ายต่างๆ ที่เห็นว่ามีความจำเป็นแก่

[104] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[105] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

การดำเนินการตามกฎหมาย และนำเสนอต่อกรรมการผู้จัดการใหญ่ ประธานกรรมการบริหาร (CEO) หรือคณะกรรมการที่เกี่ยวข้อง

3.2.5 การเข้าถึงข้อมูลที่จำเป็น

ในการทำหน้าที่กำกับดูแลและตรวจสอบได้อย่างสมบูรณ์ DPO จะต้องได้รับข้อมูล เอกสาร การเข้าถึงข้อมูล สถานที่ รหัสผ่าน ฯลฯ ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลและกิจกรรมการประมวลผลต่างๆ ของสถาบันการเงิน

จากแบบสอบถามพบว่า[106] การเข้าถึงข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมายของ DPO เป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 6 แห่ง (ขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่งสถาบันการเงินขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่สี่ และสถาบันการเงินขนาดใหญ่ 2 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้การเข้าถึงข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการเป็น *‘อันดับห้า’*

จากการสัมภาษณ์พบว่า[107] สาเหตุของปัญหาข้างต้นเกิดจากสถาบันการเงินบางแห่งอาจก่อตั้งมาแล้วเป็นระยะเวลานานหรือมีการจัดเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก โดยเฉพาะอย่างยิ่งในสถาบันการเงินขนาดใหญ่ ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่ 2 แห่งเห็นว่า เนื่องจากสถาบันการเงินก่อตั้งมาเป็นระยะเวลานาน ประกอบกับมีการจัดเก็บข้อมูลจำนวนมาก ทำให้ในบางกรณีไม่สามารถค้นหาข้อมูลส่วนบุคคลหรือกิจกรรมการประมวลผลทั้งหมดเพื่อทำหน้าที่ตามกฎหมายได้อย่างครบถ้วน เช่น ไม่สามารถปฏิบัติตามคำขอใช้สิทธิของเจ้าของข้อมูลในการแก้ไขเปลี่ยนแปลงหรือลบข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่หลากหลายแห่งภายในองค์กร

---

[106] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[107] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

3.2.6 การจ้างที่ปรึกษาซึ่งเป็นบุคคลภายนอก

เนื่องจากบางกรณีบุคลากรภายในสถาบันการเงินอาจไม่สามารถแก้ไขปัญหาในการปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้น จึงอาจต้องติดต่อขอคำปรึกษาจากบุคคลภายนอก เช่น บริษัทที่ปรึกษากฎหมาย หรือผู้เชี่ยวชาญจากมหาวิทยาลัย เป็นต้น

จากแบบสอบถามพบว่า[108] การจ้างที่ปรึกษาซึ่งเป็นบุคคลภายนอกเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 6 แห่ง (ขนาดใหญ่ 3 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่งสถาบันการเงินขนาดขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นลำดับที่หก สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นลำดับที่เจ็ด ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้การจ้างที่ปรึกษาซึ่งเป็นบุคคลภายนอกเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการเป็น *‘อันดับหก’*

จากการสัมภาษณ์[109] DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “ผู้เชี่ยวชาญที่มีความรู้ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างลึกซึ้งนั้นหายาก โดยเฉพาะอย่างยิ่งผู้ที่มีความรู้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานสากลที่ได้รับการยอมรับ ตัวอย่างเช่น ของประเทศญี่ปุ่นหรือประเทศอื่นๆ ซึ่งอยู่ใน GDPR Whitelist”

3.2.7 การประสานงานกับหน่วยงานกำกับดูแล

DPO มีหน้าที่เป็นผู้ประสานงานหลักกับหน่วยงานกำกับดูแล (เช่น ธปท. สคส.) หรือในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลอาจขอคำปรึกษาหารือที่เป็นประโยชน์จากหน่วยงานกำกับดูแล[110]

จากแบบสอบถามพบว่า[111] การประสานงานกับหน่วยงานกำกับดูแลเป็นทรัพยากรที่ถูกกล่าวถึงโดยสถาบันการเงินจำนวน 5 แห่ง (ขนาดใหญ่ 2 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่งสถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่งให้

---

[108] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[109] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[110] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคหนึ่ง (3)

[111] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่หก ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้การประสานงานกับหน่วยงานกำกับดูแลเป็นทรัพยากรที่ DPO และคณะทำงานฯ ของสถาบันการเงินต้องการเป็น 'อันดับเจ็ด'

จากการสัมภาษณ์พบว่า[112] ผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินต้องการให้เกิดความชัดเจนของข้อกฎหมายและกฎระเบียบที่กำลังจะออก เนื่องจากความไม่ชัดเจนของกฎหมายส่งผลกระทบต่อการปฏิบัติงานของพนักงานและการดำเนินธุรกิจขององค์กร โดยเจ้าหน้าที่ฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า "ถึงแม้มีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่ปัจจุบันองค์กรดังกล่าวยังไม่ได้มีลักษณะเป็นทางการ และพบว่าประเด็นทางกฎหมายที่สถาบันการเงินเคยส่งไปสอบถามยังขาดความชัดเจน อีกทั้งคำตอบของเจ้าหน้าที่สำนักงานฯ ก็ไม่ได้มีผลผูกพันทางกฎหมายเท่าใดนัก"

3.2.8 ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล

นอกเหนือจากทรัพยากรตั้งแต่หัวข้อ 3.2.1 ถึงหัวข้อ 3.2.7 ข้างต้น ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Coordinator) เป็นอีกหนึ่งบุคคลที่จะช่วยทำหน้าที่ประสานงาน แลกเปลี่ยนข้อมูล ให้ความช่วยเหลืออื่นใดที่จำเป็น รวมถึงรายงานปัญหาที่เกิดขึ้นจากการประมวลผลข้อมูลให้ DPO ทราบ[113] จึงควรสนับสนุนให้มีการแต่งตั้งผู้ประสานงานแต่ละหน่วยธุรกิจ หากสถาบันการเงินนั้นมีทรัพยากรเพียงพอ[114]

ผู้เขียนได้ทำการสัมภาษณ์สถาบันการเงินทั้ง 13 แห่งว่ามีการแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ความช่วยเหลือในการทำงานของ DPO หรือไม่ ซึ่งผลการสัมภาษณ์ปรากฏตามตารางด้านล่างนี้[115]

---

[112] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[113] ผู้เขียนเรียบเรียงจาก EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.9

[114] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[115] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 21 การแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน

การแต่งตั้งผู้ประสานงานฯ	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
แต่งตั้งแล้ว	5	1	5
ยังไม่มีการแต่งตั้งอย่างเป็นทางการ	-	1	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[116] ถึงแม้กฎหมายไม่ได้กำหนดให้มีการแต่งตั้งผู้ประสานงานดังกล่าว แต่สถาบันการเงินส่วนใหญ่ (11 แห่ง) ได้ดำเนินการแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลประจำแต่ละฝ่ายงาน[117] ซึ่งผู้ประสานงานฯ ของสถาบันการเงินแต่ละแห่งจะเป็นผู้บริหารระดับต้นหรือระดับกลางของสถาบันการเงิน บุคคลดังกล่าวมีหน้าที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลแตกต่างกันไปในแต่ละองค์กร เช่น ให้ความเห็นชอบการประมวลผลข้อมูลส่วนบุคคลเบื้องต้น บันทึกรายละเอียดของผลิตภัณฑ์หรือการให้บริการลงในรายการกิจกรรมการประมวลผลข้อมูล รายงานความคืบหน้าหรือให้ความช่วยเหลืออย่างอื่นต่อ DPO

ส่วนสถาบันการเงินที่เหลืออีก 2 แห่ง (ขนาดกลาง 1 แห่งและขนาดเล็ก 1 แห่ง) ยังไม่มีการแต่งตั้งบุคคลดังกล่าวอย่างเป็นทางการ โดยผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “พนักงานภายในองค์กรต่างให้ความร่วมมือในการปฏิบัติตามกฎหมายเนื่องจากกฎหมายกำหนดอัตราโทษไว้สูง ถึงแม้ปัจจุบันไม่มีการแต่งตั้งผู้รับผิดชอบประสานงานด้านคุ้มครองข้อมูลส่วนบุคคลโดยตรง แต่มี Compliance Champion ซึ่งทำหน้าที่กำกับตามกฎเกณฑ์ทั่วไป ซึ่งจะต้องรับผิดชอบงานกำกับตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย” ส่วน DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งให้สัมภาษณ์ว่า “อยู่ในระหว่างมอบหมายให้ดำเนินการแต่ประสบปัญหาเรื่องโรคระบาดโควิด-19 และ Work from home”

[116] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[117] ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลที่ประจำอยู่ในแต่ละฝ่ายงานภายในสถาบันการเงินมีชื่อเรียกแตกต่างกันตามแต่ละองค์กร เช่น DPO Champion, Privacy Champion, DPO Representative เป็นต้น เมื่อกฎหมายมิได้กำหนดหน้าที่ในการแต่งตั้งผู้ประสานงานดังกล่าว จึงขึ้นอยู่กับความจำเป็นและความพร้อมด้านทรัพยากรบุคคลของแต่ละสถาบันการเงิน (สถาบันการเงินขนาดใหญ่แห่งหนึ่งมีผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลประจำแต่ละหน่วยงาน หน่วยงานละมากกว่า 1 คน รวมมีผู้ประสานงานฯ ไม่ต่ำกว่า 500 คน)

3.3 ความเป็นอิสระ

ประเด็นปัญหาใหญ่อีกเรื่องหนึ่งเกี่ยวกับ DPO ที่มีการถกเถียงกันอย่างกว้างขวาง คือ สถาบันการเงินควรแต่งตั้งบุคคลภายในองค์กรหรือภายนอกองค์กรเป็น DPO โดยเฉพาะอย่างหากองค์กรเลือกที่จะแต่งตั้งบุคคลภายในองค์กรให้ทำหน้าที่เป็น DPO บุคคลนั้นควรเป็นบุคคลใดจากแผนกหรือฝ่ายงานใด และควรเป็นบุคคลในระดับใด

DPO จะต้องเข้ามาเป็นส่วนหนึ่งขององค์กร กล่าวคือ ต้องมีส่วนเกี่ยวข้องในทุกประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรอย่างเหมาะสมและทันท่วงที[118] ในขณะเดียวกัน DPO ต้องมีความเป็นอิสระในการตัดสินใจ อย่างไรก็ตาม ในทางปฏิบัติเป็นเรื่องยากที่บุคคลใดบุคคลหนึ่งซึ่งฝังตัวอยู่ภายในองค์กรใดองค์กรหนึ่งจะมีความเป็นอิสระในการตัดสินใจได้อย่างแท้จริง[119]

ตามที่เคยได้กล่าวไว้แล้วในตอนต้นของบทที่ 3 ว่าการแต่งตั้ง DPO ของสถาบันการเงินเป็นการแต่งตั้งจากพนักงานประจำภายในองค์กรทั้งหมด ดังนั้นจึงมีความเป็นไปได้ที่ DPO ของแต่ละสถาบันการเงินอาจมีผู้บังคับบัญชาโดยตรงที่มิใช่ผู้บังคับบัญชาสูงสุดของฝ่ายบริหารประจำองค์กร หรืออาจจะต้องเผชิญความกดดันจากทั้งเพื่อนร่วมงาน ผู้บังคับบัญชาโดยตรง และผู้บริหารที่มีตำแหน่งสูงกว่าตนในองค์กร เมื่อต้องดำเนินการตามภารกิจของ DPO ตามกฎหมาย การปฏิบัติงาน

[118] GDPR, Article 44(1)

[119] Centre for Information Policy Leadership (CIPL), "The Role and Function of a Data Protection Officer in Practice and in the European Commission's Proposed General Data Protection Regulation : Report on DPO Survey Results," [Online] Accessed: 14 Jan 2021. Available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf (จากผลสำรวจเรื่องบทบาทและหน้าที่ของ DPO ในทางปฏิบัติภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป DPO ท่านหนึ่งให้สัมภาษณ์ว่า DPO ทุกคนล้วนต้องมีหน้าที่ตามวัตถุประสงค์และกลยุทธ์ทางธุรกิจขององค์กร ไม่มีบุคคลมีความเป็นอิสระอย่างแท้จริง แม้แต่ประธานกรรมการบริหาร (CEO) ก็มีความรับผิดชอบต่อบอร์ด และบอร์ดก็มีหน้าที่ความรับผิดชอบต่อผู้ถือหุ้น DPO จะต้องเป็นผู้ให้คำแนะนำถึงวิธีปฏิบัติงานที่ทำให้องค์กรดำเนินธุรกิจอย่างเป็นธรรม ถูกต้องตามจรรยาบรรณ และเป็นไปตามที่กฎหมายกำหนด)

ของพนักงานภายในสถาบันการเงินที่เป็น DPO จึงอาจก่อให้เกิดความขัดแย้ง หรือผลเสียต่อเพื่อนร่วมงาน ผู้บังคับบัญชาโดยตรง หรือผู้บริหารที่มีตำแหน่งสูงกว่าตนในองค์กรได้

ในการศึกษาวิจัยประเด็นความเป็นอิสระในการตัดสินใจของ DPO ผู้เขียนจึงได้สัมภาษณ์ DPO และผู้ปฏิบัติงานที่เกี่ยวข้องของสถาบันการเงินต่างๆ ซึ่งมีคำถามที่ใช้ในการสัมภาษณ์ 4 ข้อ ได้แก่ (1) DPO สามารถปฏิบัติหน้าที่ตามกฎหมายได้โดยมีความเป็นอิสระในการทำงานและการตัดสินใจ แยกจากผู้บริหารระดับสูง/คณะกรรมการของสถาบันการเงินหรือไม่ เพราะเหตุใด (2) โดยปกติ DPO สามารถรายงานความคืบหน้า หรือปัญหาเกี่ยวกับการปฏิบัติหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยตรงต่อบุคคลใดได้บ้าง (3) มีการกำหนดวาระการรายงานไว้หรือไม่ บ่อยเพียงใด (4) ที่ผ่านมา DPO รายงานให้ผู้บริหารสูงสุด/คณะกรรมการของสถาบันการเงินในประเด็นเกี่ยวกับข้อมูลส่วนบุคคลเรื่องใดบ้าง ประมาณกี่ครั้ง และ (5) จากประสบการณ์ทำงานของท่านมีสถานการณ์ใดบ้างหรือไม่ที่ DPO ไม่สามารถรายงานโดยตรงไปยังผู้บริหารสูงสุดได้

3.3.1 สถานะ และสาเหตุของความเป็นอิสระ

เนื่องจาก DPO มีหน้าที่ให้คำแนะนำ และติดตามตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติความเห็นของฝ่ายงานต่างๆ ภายในองค์กรอาจไม่ตรงกับความเห็นของ DPO รวมถึงการทำงานของ DPO อาจจะก่อให้เกิดความยากลำบากในมุมของหน่วยงานธุรกิจ กฎหมายจึงกำหนดให้ DPO ต้องมีความเป็นอิสระ (independence) ไม่ได้รับคำสั่งใดๆ (instruction) ในประเด็นที่เกี่ยวข้องกับการปฏิบัติหน้าที่ DPO ตามกฎหมาย[120]

[120] WP29, Guidelines on DPOs. Ibid, p.15. (ตัวอย่างเช่น DPO ต้องไม่ได้รับคำสั่งเกี่ยวกับการกำหนดผลลัพธ์ของการประมวลผลข้อมูล คำสั่งกำหนดวิธีการตรวจสอบคำขอใช้สิทธิหรือคำร้องเรียนของเจ้าของข้อมูล หรือคำสั่งว่าจะต้องขอคำปรึกษาหารือกับหน่วยงานกำกับดูแลก่อนหรือไม่ นอกจากนี้ DPO จะต้องไม่ถูกครอบงำการตัดสินใจในเรื่องที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งในเรื่องของการตีความกฎหมาย)

ในเบื้องต้น ผู้เขียนได้สัมภาษณ์ DPO และผู้ปฏิบัติงานที่เกี่ยวข้องของสถาบันการเงินต่างๆ ว่า DPO สามารถปฏิบัติหน้าที่ตามกฎหมายได้โดยมีความเป็นอิสระในการทำงานและการตัดสินใจ แยกจากผู้บริหารระดับสูง/คณะกรรมการของสถาบันการเงินหรือไม่ เพราะเหตุใด

ผลการสัมภาษณ์พบว่า DPO ของสถาบันการเงินส่วนใหญ่ให้สัมภาษณ์ว่ามีความเป็นอิสระในการปฏิบัติหน้าที่และการตัดสินใจ และ DPO ของสถาบันการเงินขนาดเล็กเพียงแห่งเดียวมีความเห็นว่าการปฏิบัติงานของตนนั้นขาดความเป็นอิสระ

ตารางที่ 22 จำนวน DPO ผู้ให้สัมภาษณ์ว่ามีความเป็นอิสระในการปฏิบัติหน้าที่

ความเป็นอิสระของ DPO	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
มีความเป็นอิสระ	5	2	5
ไม่มีความเป็นอิสระ	-	-	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[121] DPO ของสถาบันการเงิน 12 แห่ง (ขนาดใหญ่ 5 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 5 แห่ง) ซึ่งให้สัมภาษณ์ว่ามีความเป็นอิสระในการปฏิบัติหน้าที่และการตัดสินใจ ระบุสาเหตุความเป็นอิสระของ DPO ที่สำคัญไว้ ดังต่อไปนี้

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง ให้เหตุผลว่า “มีความเป็นอิสระเพราะทำหน้าที่เป็น 2nd Line จึงไม่มีส่วนได้เสียกับผลประโยชน์ของการประมวลผลข้อมูลส่วนบุคคล สามารถแสดงความคิดเห็นอย่างมีเหตุผล ซึ่งที่ผ่านมาได้รับการพิจารณาและความน่าเชื่อถือจากส่วนงานต่างๆ มาโดยตลอด”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง ขนาดกลางแห่งหนึ่ง และขนาดเล็กแห่งหนึ่ง ระบุสาเหตุของความเป็นอิสระในการตัดสินใจไปในทางเดียวกันว่า “มีช่องทางรายงานตรงต่อผู้บริหารระดับสูง/คณะกรรมการที่ไม่ผ่านสายบังคับบัญชาหลัก”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง กล่าวว่า “มีการจัดตั้งหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลแยกออกมาเป็นอิสระต่างหากจากหน่วยงานอื่น” DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่ง เสริมว่า “หน่วยงานด้านการคุ้มครอง

[121] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ข้อมูลส่วนบุคคลไม่อยู่ภายใต้ฝ่ายงาน/สายงานใด และกำหนดโครงสร้างดังกล่าวไว้ในแผนผังองค์กรอย่างชัดเจน”

- ในขณะที่ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง กล่าวว่า “ถึงแม้ว่า DPO และคณะกรรมการคุ้มครองข้อมูล (ขององค์กร) แต่ละคนจะอยู่ภายใต้สายบังคับบัญชาต่างๆ มีผู้บังคับบัญชาที่มีความเป็นอิสระเป็นผู้ประเมินผลงาน แต่ได้มีการกำหนดขอบเขตและบทบาทหน้าที่ของบุคคลดังกล่าวไว้อย่างชัดเจน”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “มีความเป็นอิสระเนื่องจากดำเนินงานภายใต้คณะกรรมการอิสระ (independent director) ขององค์กร และได้รับความร่วมมือและคำแนะนำที่ดีจากผู้บริหารระดับสูงและคณะกรรมการที่เกี่ยวข้อง”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “มีแนวปฏิบัติบริหารจัดการความเป็นอิสระ เช่น หากเกิดเหตุละเมิดข้อมูลส่วนบุคคล DPO จะได้รับความช่วยเหลือจากกรรมการผู้จัดการใหญ่ให้สามารถหาข้อมูลเพื่อค้นหาข้อเท็จจริงได้ทั้งหมด”
- DPO ของสถาบันการเงินสองแห่งชี้ว่า มีฝ่ายตรวจสอบภายใน (Internal Audit) ตรวจสอบการปฏิบัติงานของ DPO และหน่วยธุรกิจ และรายงานต่อคณะกรรมการตรวจสอบซึ่งเป็นบุคคลภายนอก

ในขณะที่ DPO ของสถาบันการเงินขนาดเล็ก 1 แห่งซึ่งเป็นผู้รับผิดชอบทางด้านเทคโนโลยีสารสนเทศ มีความเห็นว่า “ตนเองขาดความเป็นอิสระ เนื่องจากในขณะที่มีการแต่งตั้งยังไม่ปรากฏประเด็นเรื่องความเป็นอิสระหรือความขัดแย้งทางผลประโยชน์” นอกจากนี้ ผู้ให้สัมภาษณ์เห็นว่าองค์กรแต่งตั้ง DPO คนใหม่บุคคลภายในที่ไม่มีงานประจำ และไม่เห็นด้วยกับการแต่งตั้งบุคคลภายนอกเป็น DPO เพราะอาจเสียค่าใช้จ่ายเป็นจำนวนมาก และใช้ระยะเวลานานกว่า DPO ที่เป็นบุคคลภายนอกจะสามารถทำความเข้าใจธุรกิจขององค์กรได้[122]

ผู้เขียนมีความเห็นว่าสิ่งที่มีความสำคัญมากที่สุดในประเด็นความเป็นอิสระในการตัดสินใจของ DPO คือ สายรายงานตรงต่อผู้บริหารระดับสูงขององค์กรที่มีความเป็นอิสระ (เช่น คณะกรรมการกำกับดูแลข้อมูล คณะกรรมการตรวจสอบ กรรมการผู้จัดการใหญ่ เป็นต้น) เนื่องจาก

[122] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ลำดับการบังคับบัญชาหรือตำแหน่งภายในองค์กรของ DPO ส่งผลต่อความเป็นอิสระในการปฏิบัติหน้าที่ โดยเฉพาะอย่างยิ่งเมื่อต้องให้คำปรึกษาต่อผู้บริหารระดับสูงทางสายงานธุรกิจหรือตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคลของสายงานทางธุรกิจ สถาบันการเงินที่ยังไม่มีการกำหนดโครงสร้างที่เหมาะสม จำเป็นต้องมีการปรับโครงสร้างขององค์กรให้สอดรับกับหลักความเป็นอิสระ โดย DPO จะต้องไม่อยู่ภายใต้บุคคลที่มีความรับผิดชอบทางธุรกิจ แต่ต้องกำหนดให้ DPO อยู่ภายใต้หน่วยงานรับผิดชอบดูแลด้านข้อมูลส่วนบุคคลที่มีกรรมการ ที่ไม่ใช่ผู้บริหารหรือกรรมการอิสระดำรงตำแหน่งเป็นผู้บังคับบัญชา และมีสายการรายงานโดยตรงระหว่าง DPO กับบุคคลดังกล่าว เพื่อให้สามารถขอคำแนะนำและขอความช่วยเหลือที่จำเป็นต่อการทำหน้าที่ตามกฎหมาย (เช่น อำนาจในการตรวจสอบหน่วยธุรกิจในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล) และกำหนดให้ฝ่ายตรวจสอบภายใน (internal audit) ตรวจสอบการทำงานของ 1st line ภายหลังจากดำเนินงานไปแล้วระยะหนึ่ง เช่น กำหนดให้ตรวจสอบปีละครั้ง

3.3.2 สายการรายงาน

DPO ต้องสามารถสามารถรายงานไปยังผู้บริหารสูงสุดขององค์กรโดยตรงได้[123] ทั้งนี้ถึงแม้ DPO จะมีสถานะเป็นเพียงลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลก็ตาม DPO จะต้องอยู่ในสภาวะที่สามารถปฏิบัติหน้าที่และภารกิจตามกฎหมายได้อย่างเป็นอิสระด้วยเช่นกัน[124]

ผู้เขียนทำการเก็บข้อมูลจากแบบสอบถามและการสัมภาษณ์ DPO ของสถาบันการเงินต่างๆ โดยใช้คำถามว่า “โดยปกติ DPO สามารถรายงานความคืบหน้า หรือปัญหาเกี่ยวกับการปฏิบัติหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยตรงต่อบุคคลใดได้บ้าง และมีการกำหนดวาระการรายงานเรื่องดังกล่าวกำหนดไว้หรือไม่ บ่อยเพียงใด”

จากแบบสอบถามพบว่า[125] สถาบันการเงินที่ได้กำหนดวาระประจำของการรายงานประเด็นเรื่องการคุ้มครองข้อมูลส่วนบุคคล เช่น รายเดือน รายไตรมาส หรือรายปี ทั้งนี้ ตามความเหมาะสมของเรื่องที่มีการรายงาน มีจำนวน 9 แห่ง (ได้แก่ สถาบันการเงินขนาดใหญ่ 4 แห่ง ขนาด

[123] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรค 3 และ GDPR, Article 38(3)

[124] GDPR, Recital 97

[125] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

กลาง 1 แห่ง และขนาดเล็ก 4 แห่ง) ส่วนสถาบันการเงินการเงินที่ไม่ได้กำหนดเป็นวาระประจำ มีจำนวน 4 แห่ง (ได้แก่ สถาบันการเงินขนาดใหญ่ 1 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 2 แห่ง)

ตารางที่ 23 สายการรายงานภายในสถาบันการเงินของ DPO ผู้ให้สัมภาษณ์

บุคคลที่ DPO รายงานถึง	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ผู้บริหารอาวุโส (senior)	3	2	4
บุคลากรระดับ c-level	3	2	3
คณะกรรมการ (committee)[126]	5	-	3
คณะกรรมการสถาบันการเงิน	3	1	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

โดยบุคคลหรือหน่วยงานที่ปัจจุบัน DPO มีสายการรายงานไปถึง เรียงลำดับจากมากที่สุดไปน้อยที่สุด ได้แก่ ผู้บริหารอาวุโส (senior management level) (9 แห่ง: สถาบันการเงินขนาดใหญ่ 2 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 4 แห่ง) บุคลากรระดับประธานเจ้าหน้าที่ (C-Level) (8 แห่ง: สถาบันการเงินขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 3 แห่ง) คณะกรรมการ (committee) (8 แห่ง: สถาบันการเงินขนาดใหญ่ 5 แห่ง และขนาดเล็ก 3 แห่ง) และคณะกรรมการของสถาบันการเงิน (board of directors) (5 แห่ง: สถาบันการเงินขนาดใหญ่ 3 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่ง)[127]

ทั้งนี้ บทบัญญัติกฎหมายที่กำหนดให้ DPO สามารถรายงานตรงต่อ “ผู้บริหารสูงสุด” ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[128] ไม่มีการให้คำนิยามไว้อย่างชัดเจนว่าบุคคลดังกล่าวหมายถึงบุคคลใดหรือหน่วยงานใดของสถาบันการเงิน ในประเด็นนี้ผู้เขียนมีความเห็นว่า DPO ต้องมีสายการรายงานตรงต่อ “บุคคลที่มีอำนาจตัดสินใจสูงสุด” ของ

[126] จากการสัมภาษณ์พบว่า คณะกรรมการภายในองค์กรที่ DPO ของสถาบันการเงิน 8 แห่งตามตารางข้างต้นกล่าวว่ามีสายการรายงานไปถึง ยกตัวอย่างเช่น คณะกรรมการคุ้มครองข้อมูล (Data Protection Committee) คณะกรรมการกำกับโครงการคุ้มครองข้อมูลส่วนบุคคล (PDPA Steering Committee) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) คณะกรรมการกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance Committee) คณะกรรมการบริหารความเสี่ยง (Risk Management Committee) และคณะกรรมการดำเนินโครงการ (Project Committee)

[127] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[128] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรค 3 และ GDPR, Article 38(3)

สถาบันการเงิน โดยบุคคลดังกล่าวอาจมีชื่อตำแหน่งที่แตกต่างกันไปตามแต่ละสถาบันการเงิน เช่น ประธานเจ้าหน้าที่บริหาร (CEO) กรรมการผู้จัดการใหญ่ (MD) หรือผู้อำนวยการสถาบันการเงิน แต่ไม่ควรรายงานไปยังคณะกรรมการของสถาบันการเงิน (board of director) เนื่องด้วยเหตุผลสองข้อ คือ (1) ข้อกฎหมายที่คุ้มครองสถานะของ DPO ไม่ว่าจะเป็นเรื่องความเป็นอิสระ การปราศจากความขัดแย้งทางผลประโยชน์ และข้อห้ามมิให้ปลดหรือลงโทษ DPO ด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตามกฎหมาย ล้วนอาจขัดกับผลประโยชน์ของสถาบันการเงินได้ และ (2) ความเสี่ยงด้านความเป็นส่วนตัว (privacy risk) ถือเป็นความเสี่ยงอย่างหนึ่งของความเสี่ยงองค์กรทั้งหมด DPO จึงควรรายงานประเด็นที่เกี่ยวข้องกับความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลต่อผู้บังคับบัญชาที่ไม่มีความเกี่ยวพันกับผลประโยชน์จากการดำเนินธุรกิจขององค์กรโดยตรง มิใช่คณะกรรมการขององค์กร (Board of Directors) ซึ่งต้องดำเนินกิจการเพื่อประโยชน์ของผู้ถือหุ้น

3.3.3 ประเด็นการคุ้มครองข้อมูลส่วนบุคคลที่มีการรายงาน

ในการแต่งตั้ง DPO สถาบันการเงินควรกำหนดอำนาจหน้าที่ให้ชัดเจนและครอบคลุมหน้าที่ตามกฎหมาย และอาจเพิ่มเติมเรื่องหน้าที่การรายงานผู้บริหารเป็นระยะหรือเฉพาะกรณีที่มีปัญหา เช่น กรณีมีความเสี่ยงที่อาจเกิดเหตุละเมิดข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ ขึ้นอยู่กับการบริหารจัดการและวัฒนธรรมของสถาบันการเงินแต่ละแห่ง[129] หาก DPO พบว่ามีบุคคลใดทั้งภายในและภายนอกองค์กรไม่ปฏิบัติตาม ให้ DPO รายงานต่อผู้บริหารระดับสูงขององค์กร ซึ่งผู้บริหารระดับสูงมีหน้าที่แก้ไข ปรับปรุง รวมไปถึงลงโทษพนักงาน หรือผู้ประมวลผลข้อมูล หรือบุคคลใดก็ตามที่ปฏิบัติหน้าที่บกพร่อง[130] นอกจากนี้ อีกเรื่องหนึ่งที่ควรมีการรายงานต่อผู้บริหารสูงสุดขององค์กร คือ จำนวนและสาระสำคัญของข้อร้องเรียนของเจ้าของข้อมูล[131]

---

[129] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[130] หากสถาบันการเงินใช้บริษัทภายนอกในการจัดเก็บข้อมูลส่วนบุคคล และพบว่าเกิดการละเมิดข้อมูลส่วนบุคคล สถาบันการเงินควรพิจารณาเปลี่ยนบริษัทจัดเก็บข้อมูล

[131] วีระ ประเสริฐนุกูล ผู้ช่วยผู้อำนวยการฝ่ายบริหารความเสี่ยงภาพรวม ธนาคารแห่งประเทศไทย, "สัมภาษณ์ เรื่อง บทบาทหน้าที่และปัญหาที่เกิดขึ้นจากการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล,"(6 สิงหาคม 2564).

ผู้เขียนได้เก็บข้อมูลจากแบบสอบถามและการสัมภาษณ์จาก DPO รวมถึงผู้ที่เกี่ยวข้องของแต่ละสถาบันการเงินว่า “ที่ผ่านมา DPO รายงานให้ผู้บริหารสูงสุด/คณะกรรมการของสถาบันการเงินในประเด็นเกี่ยวกับข้อมูลส่วนบุคคลเรื่องใดบ้าง ประมาณกี่ครั้ง”

จากการสำรวจพบว่า[132] ประเด็นการคุ้มครองข้อมูลส่วนบุคคลที่ DPO รายงานต่อผู้บริหารสูงสุด ได้แก่ ความคืบหน้าในการปฏิบัติตามกฎหมาย แผนการดำเนินงานด้านข้อมูลส่วนบุคคล งบประมาณด้านการคุ้มครองข้อมูลส่วนบุคคล ข้อร้องเรียนของเจ้าของข้อมูล เหตุการณ์ที่อาจเข้าข่ายละเมิดข้อมูลส่วนบุคคล และ หลักเกณฑ์การบริหารความเสี่ยงข้อมูลส่วนบุคคล ซึ่งแต่ละประเด็นที่มีการรายงานดังกล่าวมีจำนวนครั้งโดยเฉลี่ย ปรากฏดังตารางด้านล่างนี้

ตารางที่ 24 จำนวนครั้งโดยเฉลี่ยของการรายงานประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคลไปยังผู้บริหารระดับสูง/คณะกรรมการภายในสถาบันการเงิน[133]

ประเด็นที่มีการรายงานต่อผู้บริหารระดับสูง/ คณะกรรมการภายในสถาบันการเงิน	ขนาดใหญ่ (ครั้ง)	ขนาดกลาง (ครั้ง)	ขนาดเล็ก (ครั้ง)
ความคืบหน้าในการปฏิบัติตามกฎหมาย	10	8	11
แผนการดำเนินงานด้านข้อมูลส่วนบุคคล	8	18	8
งบประมาณที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล	3	3	2
ข้อร้องเรียนของเจ้าของข้อมูลส่วนบุคคล	3	-	4
เหตุการณ์ที่อาจเข้าข่ายละเมิดข้อมูลส่วนบุคคล[134]	-	-	2
หลักเกณฑ์การบริหารความเสี่ยงของข้อมูลส่วนบุคคล	2	-	-

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

นอกเหนือจากการรายงานตามประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคลตามตารางข้างต้น ปัจจุบันมีร่างกฎหมายที่ช่วยรับรองความเป็นอิสระในการตัดสินใจของ DPO ซึ่งกำหนดให้ “ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องดำเนินงานโดยคำนึงถึงความเห็นและคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามสมควร ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่เห็นด้วยหรือไม่ปฏิบัติตามคำแนะนำของ DPO ให้ DPO บันทึกข้อเท็จจริงและ

[132] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[133] ทั้งนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินบางแห่งไม่สามารถระบุจำนวนครั้งของการรายงานดังกล่าวได้

[134] จากการสัมภาษณ์พบว่า DPO รายงานไปยังผู้บริหารระดับสูง/คณะกรรมการของสถาบันการเงินว่าไม่มีเหตุละเมิดฯ เกิดขึ้น

ระบุเหตุผลของการตัดสินใจไว้ รวมถึงระบุผู้มีส่วนร่วมในการตัดสินใจหรืออนุมัติการดำเนินการดังกล่าวและทำบันทึกรายงานเพื่อแจ้งแก่ผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคล”[135] จะเห็นได้ว่า ปัญหาที่ผู้ควบคุมหรือผู้ประมวลผลไม่เห็นด้วยหรือไม่ปฏิบัติตามคำแนะนำของ DPO จึงเป็นอีกประเด็นหนึ่งที่ควรมีการรายงานตรงต่อผู้บริหารสูงสุดของสถาบันการเงิน[136]

3.3.4 สถานการณ์ที่ไม่สามารถรายงานได้

เนื่องจากการแต่งตั้ง DPO ของธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจซึ่งเป็นกลุ่มเป้าหมายของผู้สัมภาษณ์เป็นการแต่งตั้ง DPO จากพนักงานประจำภายในองค์กรทุกแห่ง จึงมีความเป็นไปได้ว่า DPO ของสถาบันการเงินต่างๆ อาจจะต้องเผชิญความกดดันจากเพื่อนร่วมงานหรืออาจอยู่ในสายบังคับบัญชาหรือมีการสายรายงานที่ไม่เหมาะกับการปฏิบัติหน้าที่ตรวจสอบการประมวลผลข้อมูลส่วนบุคคลขององค์กร อันจะนำมาซึ่งความไม่เป็นอิสระในการปฏิบัติงานของ DPO

ในการศึกษาวิจัยประเด็นดังกล่าว ผู้เขียนได้สัมภาษณ์ DPO ของสถาบันการเงินแต่ละแห่งว่า จากประสบการณ์ทำงานของ DPO แต่ละท่านมีสถานการณ์ใดบ้างหรือไม่ที่ DPO ไม่สามารถรายงานโดยตรงไปยังผู้บริหารสูงสุดขององค์กร โดยผลการสัมภาษณ์พบว่า[137] ที่ผ่านมายังไม่มีสถานการณ์ใดที่ DPO ของแต่ละสถาบันการเงินไม่สามารถรายงานโดยตรงไปยังผู้บริหารระดับสูงและคณะกรรมการได้ หากมีความจำเป็นต้องรายงานผู้บริหารระดับสูงหรือคณะกรรมการของสถาบันการเงินล้วนสามารถทำได้

ประเด็นข้างต้น ผู้เขียนเห็นว่าอาจเป็นเพราะ DPO ของภาคสถาบันการเงินโดยเฉพาะอย่างยิ่งในธนาคารพาณิชย์และสถาบันการเงินเฉพาะกิจส่วนใหญ่ในประเทศไทย ล้วนเป็นการคัดเลือกจากบุคลากรผู้บริหารระดับกลางค่อนไปทางระดับสูง โดยมีคณะกรรมการผู้บริหารของ

---

[135] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.11. โปรดดู https://www.law.chula.ac.th/event/10941/

[136] หากมีเหตุอันควรเชื่อว่าผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลของสถาบันการเงินอาจมีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่ส่งผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล นอกจากการรายงานต่อผู้บริหารสูงสุดของสถาบันการเงิน DPO ยังอาจแจ้งต่อสำนักงานเพื่อให้ดำเนินการตรวจสอบได้

[137] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

องค์กรพิจารณาให้ความเห็นชอบ จึงไม่เกิดปัญหาที่ไม่สามารถเสนอเรื่องไปยังบุคคลดังกล่าว ประกอบกับการเลื่อนการบังคับใช้ของกฎหมาย อาจเป็นอีกสาเหตุหนึ่งที่ DPO ของสถาบันการเงินยังไม่พบปัญหาดังกล่าว

3.4 ความขัดแย้งทางผลประโยชน์

ความขัดแย้งทางผลประโยชน์ (Conflict of interest) ในบทบาทหน้าที่ของ DPO ซึ่งเป็นบุคคลภายในองค์กร เป็นอีกหนึ่งปัญหาที่มีความสำคัญที่สุดและมีความสัมพันธ์กับความเป็นอิสระตามที่ได้กล่าวไว้ใน “หัวข้อ 3.3 ความเป็นอิสระ” โดยเรื่องความขัดแย้งทางผลประโยชน์ของ DPO มีกฎหมายกำหนดว่า DPO อาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ตราบเท่าที่หน้าที่หรือภารกิจนั้นไม่ขัดหรือแย้งกับการปฏิบัติหน้าที่ตามกฎหมาย[138] อย่างไรก็ดีไม่ว่า GDPR หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ต่างไม่ได้ให้คำนิยามของความขัดแย้งทางผลประโยชน์ไว้ จึงอาจทำให้เกิดปัญหาในการตีความกฎหมายได้

ความหมายโดยทั่วไปของคำว่า “ความขัดแย้งทางผลประโยชน์” (หรือ “ผลประโยชน์ทับซ้อน”) หมายถึง “สถานการณ์หรือการกระทำที่บุคคลใดบุคคลหนึ่งมีผลประโยชน์ส่วนบุคคล[139] มากพอจนเห็นได้ว่าผลประโยชน์ดังกล่าวกระทบต่อการตัดสินใจหรือการใช้วิจารณญาณในทางใดทางหนึ่งอย่างเป็นกลาง ไม่ว่าผลประโยชน์นั้นจะเป็นตัวเงินหรือผลประโยชน์ในรูปแบบอื่น” [Michael McDonald, 2016] องค์กรเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (OECD) ได้จำแนกความขัดแย้งทางผลประโยชน์ออกเป็น 3 ประเภท[140] ได้แก่

[138] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคท้าย และ GDPR, Article 38(6)

[139] ผลประโยชน์ส่วนบุคคล (private interest) เป็นผลตอบแทนที่บุคคลได้รับ โดยเห็นว่ามีคุณค่าที่จะสนองตอบความต้องการของตนเองหรือของกลุ่มที่ตนเองเกี่ยวข้อง ผลประโยชน์เป็นสิ่งจูงใจให้คนเรามีพฤติกรรมต่างๆ เพื่อสนองความต้องการทั้งหลาย (เพ็ญศรี วายวานนท์, 2527:154)

[140] สำนักงานคณะกรรมการนโยบายวิทยาศาสตร์เทคโนโลยีและนวัตกรรมแห่งชาติ, คู่มือป้องกันผลประโยชน์ทับซ้อน (Conflict of Interest) (2561), หน้า.4-5.

1) ความขัดแย้งทางผลประโยชน์ที่เกิดขึ้นจริง (actual) เกิดขึ้นเมื่อบุคคลใดบุคคลหนึ่งมีผลประโยชน์สองประการที่ขัดแย้งกัน อันมีลักษณะเป็นการขัดขวางหรือบ่อนทำลายความสามารถในการปฏิบัติตามหน้าที่และความรับผิดชอบของบุคคลนั้น[141]
2) ความขัดแย้งทางผลประโยชน์ที่เห็นกัน (perceived) เป็นกรณีผลประโยชน์ขัดกันที่ที่ปัจเจกชนเห็นว่ามีแต่แท้จริงอาจจะไม่มีก็ได้ และถึงแม้จะไม่มีอยู่จริง หากไม่มีวิธีการจัดการอย่างมีประสิทธิภาพอาจนำมาซึ่งผลเสียไม่ต่างจากกรณีความขัดแย้งทางผลประโยชน์ที่เกิดขึ้นจริง ข้อนี้แสดงให้เห็นว่า บุคคลต้องต้องปฏิบัติหน้าที่อย่างมีจริยธรรมไปพร้อมกับการทำให้ผู้อื่นรับรู้และเห็นด้วยว่าไม่ได้รับประโยชน์เช่นนั้นจริง[142]
3) ความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นได้ (potential) หมายถึง กรณีที่ผลประโยชน์ส่วนบุคคลที่มีในปัจจุบันอาจจะขัดแย้งกับผลประโยชน์ของตนที่อาจมีขึ้นในอนาคต[143]

นอกจากนี้ ความขัดแย้งทางผลประโยชน์อาจรวมถึงกรณีความขัดแย้งระหว่างหน้าที่ (conflict of duties) ซึ่งเกิดจากการที่บุคคลใดบุคคลหนึ่งมีบทบาทหน้าที่มากกว่าหนึ่งหน้าที่ ความขัดแย้งจะเกิดขึ้นเมื่อไม่สามารถแยกแยะบทบาทหน้าที่ทั้งสองออกจากกันได้ อาจทำให้การทำงานไม่มีประสิทธิภาพ หรือเกิดความผิดพลาด หรือผิดกฎหมาย ปกติหน่วยงานมักมีกลไกป้องกันปัญหานี้โดยแยกแยะบทบาทหน้าที่ต่างๆ ให้ชัดเจน แต่ก็ยังมีปัญหาได้โดยเฉพาะอย่างยิ่งในหน่วยงานที่มีกำลังคนน้อยหรือมีบุคคลเพียงบางคนเท่านั้นที่สามารถทำงานบางอย่างที่คนอื่นๆ ทำไม่ได้[144]

สำหรับบริบทของการปฏิบัติหน้าที่ DPO ตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล WP29 มีความเห็นว่าการที่ DPO สามารถปฏิบัติหน้าที่ได้โดยปราศจากความขัดแย้งทางผลประโยชน์ หมายถึง การไม่มีส่วนเกี่ยวข้องกับการกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล

---

[141] Ryerson University, "GUIDELINES FOR MANAGING REAL, POTENTIAL, AND PERCEIVED CONFLICTS OF INTEREST," [Online] Accessed: 17 Jan 2564. Available from: https://www.ryerson.ca/content/dam/research/documents/ethics/guidelines-for-managing-real-potential-and-perceived-conflicts-of-interest.pdf

[142] Ryerson University. Ibid.

[143] Ryerson University. Ibid.

[144] ผู้เขียนดัดแปลงจาก สำนักงานคณะกรรมการนโยบายวิทยาศาสตร์เทคโนโลยีและนวัตกรรมแห่งชาติ. คู่มือป้องกันผลประโยชน์ทับซ้อน (Conflict of Interest). เรื่องเดิม. หน้า.5.

และไม่สามารถดำรงตำแหน่งระดับผู้บริหารอาวุโส (senior management position) เช่น หัวหน้าฝ่ายบริหาร หัวหน้าฝ่ายดำเนินการ หัวหน้าฝ่ายการเงิน หัวหน้าฝ่ายการตลาด หัวหน้าฝ่ายทรัพยากรบุคคล หรือหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ รวมถึงตำแหน่งอื่นใดในระดับที่ต่ำกว่าระดับผู้บริหารอาวุโสในโครงสร้างองค์กรที่มีบทบาทหน้าที่อันจะนำไปสู่การตัดสินใจวัตถุประสงค์และวิธีการประมวลผลข้อมูล[145] ทั้งนี้ การเรียกชื่อตำแหน่งบางตำแหน่งไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่จะได้รับตำแหน่งนั้นจะสามารถเป็น DPO ไปด้วยในขณะเดียวกันได้หรือไม่ แต่จะต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวว่ามีความขัดแย้งทางผลประโยชน์หรือไม่

3.4.1 การพิจารณาแต่งตั้ง DPO ของสถาบันการเงิน

เพื่อป้องกันไม่ให้เกิดความขัดแย้งทางผลประโยขน์ องค์กรอาจกำหนดระเบียบหรือกฎเกณฑ์ภายใน เพื่อระบุว่าบุคคลที่มีตำแหน่งทางธุรกิจหรือมีความรับผิดชอบทางด้านใดสามารถเป็น DPO และบุคคลไม่สามารถเป็น DPO ได้[146] ผู้เขียนจึงได้ทำการสัมภาษณ์ DPO และคณะทำงานฯ ของสถาบันการเงินทั้ง 13 แห่งว่า สถาบันการเงินแต่ละแห่งมีการกำหนดว่าบุคคลซึ่งมีตำแหน่งทางธุรกิจหรือมีความรับผิดชอบทางด้านใดสามารถเป็น DPO หรือไม่สามารถเป็น DPO ได้หรือไม่อย่างไรบ้าง

จากการสัมภาษณ์พบว่า เนื่องจากกฎหมายไม่ได้กำหนดความรู้ความสามารถหรือคุณสมบัติของ DPO ไว้อย่างชัดเจน เพียงแต่ห้ามมิให้หน้าที่การปฏิบัติหน้าที่หรือภารกิจอื่นของบุคคลที่เป็น DPO ขัดแย้งกับหน้าที่ตามกฎหมาย[147] สถาบันการเงินแต่ละแห่งจึงยังไม่ได้กำหนดเกณฑ์การคัดเลือกคุณสมบัติและลักษณะต้องห้ามไว้อย่างชัดเจน ส่วนในทางปฏิบัติ การคัดเลือก DPO ของสถาบันการเงินแต่ละแห่งจะถูกกำหนดไว้อยู่ในวาระการประชุม โดยมีคณะกรรมการผู้บริหารหรือ

[145] WP29, Guidelines on DPOs. Ibid, p.16.

[146] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.10.

[147] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรคท้าย

คณะกรรมการของสถาบันการเงินเป็นผู้พิจารณาคุณลักษณะของบุคคลที่จะดำรงตำแหน่ง DPO ลักษณะของการพิจารณาแต่งตั้งบุคคลใดเป็น DPO มีดังต่อไปนี้[148]

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Committee) ซึ่งมีหน้าที่ความรับผิดชอบเป็น 2nd line หรือ 3rd line กำหนดว่า DPO ต้องมีความเป็นอิสระ” โดย DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งกล่าวว่า “บุคคลที่จะดำรงตำแหน่ง DPO ต้องมีความเป็นอิสระ ไม่มีอำนาจตัดสินใจการใช้ข้อมูล กล่าวคือ DPO ต้องไม่ใช่บุคคลที่มาจากหน่วยงานซึ่งทำหน้าที่ 1st line หรือ 3rd line ขณะที่มีการแต่งตั้ง”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “ในทางปฏิบัติบุคคลที่องค์กรจะแต่งตั้งให้ดำรงตำแหน่ง DPO จะเป็นผู้ปฏิบัติงานเบื้องหลัง (back office) ที่ไม่มีความเกี่ยวข้องกับลูกค้าโดยตรง และไม่มีตำแหน่งทางธุรกิจอยู่แล้ว จึงไม่ได้มีการกำหนดเกณฑ์ในการพิจารณาว่าบุคคลซึ่งมีตำแหน่งทางธุรกิจหรือมีความรับผิดชอบทางด้านใดสามารถเป็น DPO หรือไม่สามารถเป็น DPO ได้”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “บรรดาผู้บริหารคัดเลือกจากฝ่าย IT ฝ่ายบริหารความเสี่ยง ฝ่าย Compliance และฝ่ายกฎหมาย ท้ายที่สุดกรรมการผู้จัดการมีข้อสรุปว่าฝ่ายงานที่เหมาะสมกับตำแหน่ง DPO คือฝ่ายงาน IT เพราะมีความเชื่อมโยงกับการกำกับดูแลข้อมูล (Data Governance) แต่ในอนาคตอาจมีการเสนอหรือทบทวนกันใหม่”

ผู้เขียนเห็นว่าสถาบันการเงินแต่ละแห่งควรกำหนดเกณฑ์ในการพิจารณาบทบาทหน้าที่ของบุคคลที่จะเข้ารับตำแหน่ง DPO ไว้เป็นลายลักษณ์อักษรอย่างชัดเจน โดยจะต้องไม่เป็นผู้ที่มีอำนาจตัดสินใจวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลขององค์กร ในการพิจารณาต้องยึดหลักการ Three Lines of Defense เป็นสำคัญ ทั้งขณะที่มีการแต่งตั้งและภายหลังจากการแต่งตั้ง ซึ่งอาจคัดเลือกจากบุคคลที่มาจากหน่วยงานซึ่งทำหน้าที่ 2nd Line หรือบุคคลที่มีความรับผิดชอบเกี่ยวกับการตรวจ (เช่น ธนาคารพาณิชย์อาจแต่งตั้งจากฝ่าย compliance หรือสถาบันการเงินเฉพาะกิจอาจแต่งตั้งผู้ตรวจการธนาคารเป็น DPO เป็นต้น) หรือผู้ปฏิบัติงานเบื้องหลังที่ไม่มี

[148] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ความสัมพันธ์กับลูกค้าโดยตรง (back office) และหากภายหลังปรากฏว่าบุคคลที่ได้รับการแต่งตั้งเป็น DPO ต้องทำงานที่เกี่ยวข้องกับการตัดสินใจใช้ข้อมูลเพื่อวัตถุประสงค์ทางธุรกิจ สถาบันการเงินไม่ควรให้บุคคลนั้นทำหน้าที่เป็น DPO อีกต่อไป และต้องพิจารณาบุคคลอื่นขึ้นทำหน้าที่แทนโดยทันที อนึ่งการแต่งตั้งบุคคลภายนอกเพื่อหลีกเลี่ยงปัญหาเรื่องความขัดแย้งทางผลประโยชน์อาจไม่ใช่ทางเลือกที่เหมาะสมสำหรับสถาบันการเงินบางแห่ง เนื่องจากบุคคลภายนอกอาจขาดความรู้ความเข้าใจในวัฒนธรรม ผลิตภัณฑ์ รูปแบบการให้บริการ และดำเนินกิจกรรมประมวลผลข้อมูลขององค์กร

3.4.2 กรณีที่สถาบันการเงินประมวลผลข้อมูลส่วนบุคคลของ DPO

นอกเหนือจากความขัดแย้งทางผลประโยชน์ที่เกิดขึ้นจากบุคคลที่ทำหน้าที่เป็น DPO อำนาจตัดสินใจเกี่ยวกับวัตถุประสงค์หรือการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรแล้ว หาก DPO เป็นเจ้าของข้อมูลส่วนบุคคลและมีเหตุอันสมควรเชื่อว่าสถาบันการเงินทำการประมวลผลข้อมูลส่วนบุคคลนั้นโดยมิชอบด้วยกฎหมาย ก็เป็นอีกกรณีหนึ่งที่ทำให้ DPO ตกอยู่ในสถานะที่มีความขัดแย้งทางผลประโยชน์ได้[149]

ผู้เขียนจึงได้สัมภาษณ์ DPO ของสถาบันการเงินแต่ละแห่งเกี่ยวกับวิธีจัดการเมื่อเกิดเหตุการณ์ในลักษณะดังกล่าว โดยใช้คำถามว่า “ในกรณีที่ DPO เป็นเจ้าของข้อมูลส่วนบุคคล และเห็นว่าสถาบันการเงินที่ตนดำรงตำแหน่งอยู่ทำการประมวลผลข้อมูลส่วนบุคคลของตนโดยไม่ชอบด้วยกฎหมาย ท่านมีความเห็นว่าหากทักท้วงแล้วองค์กรไม่ดำเนินการแก้ไขให้ DPO ควรทำอย่างไรและในทางปฏิบัติเป็นไปได้หรือไม่ที่จะดำเนินการร้องเรียนต่อหน่วยงานกำกับดูแล”

ตารางที่ 25 ความเห็นของผู้ให้สัมภาษณ์เกี่ยวกับกรณีที่สถาบันการเงินประมวลผลข้อมูลส่วนบุคคลของ DPO โดยมิชอบด้วยกฎหมาย

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ไม่มีความจำเป็นต้องเสนอต่อหน่วยงานกำกับดูแล	2	1	3
จำเป็นต้องเสนอหรือร่วมหารือกับหน่วยงานกำกับดูแล	2	1	2
โดยสภาพไม่สามารถเสนอต่อหน่วยงานกำกับดูแลได้	1	-	1

[149] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.11.

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[150] ความเห็นแนวที่หนึ่ง ผู้ให้สัมภาษณ์จากสถาบันการเงินจำนวน 6 แห่ง (ขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 3 แห่ง) มีความเห็นว่าเนื่องจากสถาบันการเงินมีหน้าที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด หาก DPO (หรือแม้แต่เจ้าของข้อมูล) ทักท้วงกรณีที่สถาบันการเงินประมวลผลข้อมูลส่วนบุคคลของตนโดยมิชอบด้วยกฎหมาย ย่อมได้รับความร่วมมือจากสถาบันการเงิน และไม่มีความจำเป็นต้องร้องเรียนต่อหน่วยงานกำกับดูแล โดยให้เหตุผลที่สำคัญดังต่อไปนี้[151]

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “ด้วยวัฒนธรรมขององค์กรที่เปิดให้บุคคลต่างๆ แสดงความคิดเห็นได้อย่างเต็มที่ ประกอบกับผู้บริหารระดับสูงต่างให้ความสำคัญกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ความร่วมมือ และความช่วยเหลือที่ดีมาโดยตลอด ฉะนั้นเมื่อมีการเสนอเรื่องการประมวลผลข้อมูลส่วนบุคคลที่มิชอบด้วยกฎหมายก็ไม่น่าจะพบปัญหาดังกล่าว ฉะนั้น จึงไม่มีความจำเป็นต้องร้องเรียนต่อหน่วยงานกำกับดูแล”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “ถ้าการทักท้วงของ DPO ในฐานะที่เป็นเจ้าของข้อมูลมีการชี้แจงเหตุผลอย่างเหมาะสมว่าสถาบันการเงินต้องหยุดการประมวลผลข้อมูลนั้นเพราะเหตุใด กรณีดังกล่าวเป็นการละเมิดอย่างไร ย่อมมีน้ำหนักได้รับการพิจารณาและได้รับแก้ไขให้ถูกต้อง จึงไม่มีความจำเป็นต้องร้องเรียนหน่วยงานกำกับดูแล”
- เจ้าหน้าที่อาวุโสฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “มีโอกาสที่สถาบันการเงินจะจัดเก็บหรือประมวลข้อมูลโดยมิชอบโดยเฉพาะอย่างยิ่งหากเป็นเรื่องที่เกิดขึ้นก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ แต่ถึงแม้การประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินนั้นอาจไม่ชอบด้วยกฎหมาย แต่สถาบันการเงินก็มิได้มีเจตนาทุจริตหรือแสวงหาผลประโยชน์โดยมิชอบ จึงไม่จำเป็นที่ DPO จะต้องไปขอให้หน่วยงานกำกับดูแลดำเนินการแก้ไขให้”

[150] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[151] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ความเห็นแนวที่สอง ผู้ให้สัมภาษณ์จากสถาบันการเงินจำนวน 5 แห่ง (ขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 2 แห่ง) มีความเห็นว่ามีความเป็นไปได้ที่จะเกิดกรณีที่สถาบันการเงินไม่ดำเนินการตามคำร้องเรียนหรือคำทักท้วงนั้น และมีความจำเป็นต้องเสนอหรือร่วมหารือกับหน่วยงานกำกับดูแลเพื่อทำการแก้ไขปัญหาต่อไป โดยให้เหตุผลที่สำคัญดังต่อไปนี้[152]

- เจ้าหน้าที่ซึ่งอยู่ในคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “ต้องดำเนินการนำเสนอปัญหาไปยัง President หรือ Executive committee ซึ่งประกอบด้วยสมาชิกคณะกรรมการของสถาบันการเงิน หากยังไม่มีข้อสิ้นสุด ต้องนำวาระเข้าสู่การประชุมร่วมหารือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล”
- DPO ของสถาบันการเงินขนาดเล็กหนึ่งเห็นว่า “ในกรณีที่เป็นเจ้าของข้อมูลส่วนบุคคล ก็จะไม่อยู่ในฐานะเป็น DPO ผู้ปฏิบัติงานขององค์กรจะสามารถแยกความเป็นตัวตน และการปฏิบัติหน้าที่ในฐานะ DPO ออกจากกันได้ โดยไม่มีประเด็นทางความขัดแย้งทางผลประโยชน์ ทั้งนี้ หากทักท้วงแล้วไม่ได้รับความร่วมมือก็สามารถร้องเรียนให้หน่วยงานกำกับดูแลทราบได้”
- DPO ของสถาบันการเงินขนาดเล็กหนึ่งเห็นว่า “ถ้าทักท้วงแล้วไม่ดำเนินการให้ก็ต้องแจ้งให้ธนาคารแห่งประเทศไทยทราบ” ประกอบกับยกตัวอย่างกรณีที่หน่วยงานสหภาพของสถาบันการเงินตนร้องเรียนไปยังหน่วยงานกำกับเมื่อองค์กรไม่ตอบสนอง

ความเห็นแนวที่สาม ผู้ให้สัมภาษณ์จากสถาบันการเงินจำนวน 2 แห่ง (ขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่ง) มีความเห็นว่าเนื่องจากโดยตำแหน่ง DPO มีสถานะเป็นลูกจ้างหรือพนักงานคนหนึ่งของสถาบันการเงินที่ตนได้รับการแต่งตั้งจึงไม่สามารถดำเนินการตามกระบวนการร้องเรียนต่อหน่วยงานกำกับดูแลได้[153] ซึ่งเป็นไปทางเดียวกับที่เจ้าหน้าที่ท่านหนึ่งของสำนักงานปลัดกระทรวงดิจิทัลฯ ได้ให้สัมภาษณ์ว่า “DPO ในฐานะเจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการ

[152] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[153] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตามสิทธิที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยการร้องเรียนคณะกรรมการผู้เชี่ยวชาญตามมาตรา 73 แต่ควรคำนึงถึงความสัมพันธ์ระหว่างนายจ้างและลูกจ้างประกอบ”[154]

จากการวิเคราะห์บทบัญญัติแห่งกฎหมาย แนวปฏิบัติที่เกี่ยวข้อง ตลอดจนความเห็นและคำแนะนำของผู้ให้สัมภาษณ์แต่ละท่าน ผู้เขียนมีความเห็นว่าในกรณีที่สถาบันการเงินประมวลผลข้อมูลส่วนบุคคลโดยมีความเสี่ยงว่าการประมวลผลนั้นอาจไม่ชอบด้วยกฎหมาย ไม่ว่าเจ้าของข้อมูล (data subject) คนนั้นจะเป็น DPO หรือเป็นบุคคลอื่นใดก็ตาม สถาบันการเงินควรเร่งประสานงานกับผู้ร้องเรียนเพื่อพิจารณาว่าข้อร้องเรียนเรื่องการประมวลผลโดยมิชอบด้วยกฎหมายของบุคคลดังกล่าวสมเหตุสมผลหรือไม่ (เช่น การประมวลผลข้อมูลส่วนบุคคลเป็นการละเมิดหรือไม่ ตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล หรือตามกฎหมายอื่นใด) หากการประมวลผลข้อมูลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลที่มิชอบด้วยกฎหมายตามที่ผู้ร้องกล่าวอ้างจริง การประมวลผลที่มิชอบดังกล่าวมีความร้ายแรงมากน้อยเพียงใด ส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างไร เพื่อให้ฝ่ายงานที่เกี่ยวข้องพิจารณาแนวทางเยียวยาผู้ที่ได้รับผลกระทบจากการประมวลผลข้อมูลที่มิชอบด้วยกฎหมายนั้นต่อไป

ทั้งนี้ หากสถาบันการเงินไม่ตอบสนอง หรือพิจารณาเรื่องไว้แล้วแต่ยังไม่ได้ข้อสรุปที่เป็นที่สิ้นสุด หรือการแก้ไขเยียวยาได้ผลลัพธ์ที่ไม่น่าพอใจ เจ้าของข้อมูลควรร้องเรียนต่อหน่วยงานกำกับดูแลเพื่อขอความช่วยเหลือต่อไป อย่างไรก็ดี กรณีของ DPO อาจไม่สามารถดำเนินการตามกระบวนการร้องเรียนได้ในบางกรณี เนื่องจากมีความสัมพันธ์ระหว่างนายจ้างกับลูกจ้างต่อสถาบันการเงินที่ตนได้รับการแต่งตั้ง แต่การไม่ตอบสนองหรือไม่ดำเนินการแก้ไขเยียวยาเจ้าของข้อมูลอย่างเหมาะสม น่าจะเกิดขึ้นได้ยากโดยเฉพาะอย่างยิ่งในบริบทของสถาบันการเงิน เนื่องจากอยู่ภายใต้การกำกับดูแลอย่างเข้มงวดของหน่วยงานที่เกี่ยวข้อง ประกอบกับกฎหมายได้มีการกำหนดให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลมีความรับผิดทางแพ่ง (มาตรา 77) ให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลและกรรมการ/ผู้จัดการของนิติบุคคลมีความรับผิดทางอาญา (มาตรา 79 และมาตรา 81) ตลอดจนกำหนดโทษปรับทางปกครอง (มาตรา 82 ถึงมาตรา 90) ไว้อย่างรุนแรงตามแต่ละกรณี

[154] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

3.4.3 ความทับซ้อนระหว่างหน้าที่คุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลกับหน้าที่ที่ DPO มีต่อสถาบันการเงิน

เมื่อคำนึงถึงบทบาทหน้าที่ DPO ซึ่งเป็นบุคคลภายในสถาบันการเงินจะเห็นว่า DPO มีหน้าที่หรือภารกิจต่อสถาบันการเงินที่ได้รับการแต่งตั้ง และในขณะเดียวกันบุคคลที่เป็น DPO ก็มีหน้าที่ต้องคุ้มครองข้อมูลส่วนบุคคลเพื่อประโยชน์ของเจ้าของข้อมูลด้วย จึงอาจทำให้เกิดประเด็นเรื่องความขัดแย้งในบทบาทหน้าที่ (Conflict of Duties) ในกรณีนี้ European Data Protection Supervisor (EDPS) ได้ให้คำแนะนำว่า DPO ไม่ควรทำหน้าที่เป็นตัวแทนหรือเป็นพยานในการพิจารณาคดีการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับองค์กรที่ DPO ได้รับการแต่งตั้ง[155]

ในการค้นหาแนวทางป้องกันและหลีกเลี่ยงความขัดแย้งทางผลประโยชน์ ผู้เขียนจึงได้สอบถามความคิดเห็นของ DPO และบุคคลที่เกี่ยวข้องของแต่ละสถาบันการเงินว่า มีความเห็นอย่างไรหากมีกฎระเบียบหรือข้อบังคับกำหนดให้ ในกรณีที่ถ้าสถาบันการเงินถูกฟ้องเป็นจำเลยในคดีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล จะให้ DPO เข้ามาเป็นตัวแทนขององค์กรหรือเป็นพยานในการพิจารณาคดีไม่ได้

ตารางที่ 26 ความเห็นของผู้ให้สัมภาษณ์เกี่ยวกับการเป็นตัวแทนหรือพยานของสถาบันการเงินของ DPO

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
DPO สามารถเป็นตัวแทน/พยานของสถาบันการเงินที่ตนได้รับการแต่งตั้ง	5	2	5
DPO ไม่ควรเป็นตัวแทน/พยานของสถาบันการเงินที่ตนได้รับการแต่งตั้ง	-	-	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากผลการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงินส่วนใหญ่ (12 แห่ง) มีความเห็นที่แตกต่างออกไปจากคำแนะนำของ EDPS ข้างต้นโดยสิ้นเชิง กล่าวคือ เห็นด้วยกับการให้

[155] EDPS, Position paper on the role of Data Protection Officers of the EU institutions and bodies. September 30, 2018. pp.11-12

DPO เป็นตัวแทนของสถาบันการเงินในการพิจารณาคดี และไม่ควรตัด DPO ออกจากพยานในคดีคุ้มครองข้อมูลส่วนบุคคล โดยมีความเห็นที่สำคัญ ดังนี้[156]

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “DPO เป็นบุคคลที่รับทราบและเข้าใจข้อเท็จจริงเกิดขึ้นในองค์กร จึงไม่ควรมีกฎหมายกำหนดห้าม ในทางตรงข้าม DPO ควรจะเป็นหนึ่งในบุคคลที่ควรมาให้การต่อศาลโดยเฉพาะอย่างยิ่งถ้า DPO เป็นประจักษ์พยานที่พบเห็นหรือเกี่ยวข้องกับเหตุการณ์นั้นโดยตรง” และได้ให้ข้อสังเกตที่ว่ากรณีที่ DPO เห็นว่าคำให้การของตนจะกระทบต่อหน้าที่การงานย่อมแสดงว่า DPO ผู้นั้นขาดความเป็นอิสระ
- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “DPO เป็นผู้ปฏิบัติงานในฐานะ 2nd Line of Defense ดังนั้นในกรณีที่มีคดีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล DPO ควรจะมีส่วนเกี่ยวข้องในการชี้แจงตามขอบเขตงานของตน”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “กฎหมายกำหนดให้ DPO มีหน้าที่ให้คำปรึกษาและตรวจสอบการประมวลผลขององค์กรให้เป็นไปตามกฎหมาย และเป็นช่องทางการติดต่อ (contact point) หรือการขอใช้สิทธิของเจ้าของข้อมูล DPO จึงเปรียบเสมือน ‘ตำรวจบ้าน’ แต่ไม่ใช่คนกลางของเจ้าของข้อมูล” เจ้าหน้าที่ฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งเสริมว่า “กฎหมายเรื่องเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่ได้มีเจตนารมณ์เพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูล สังเกตได้จากการที่ไม่มีบทกฎหมายสันนิษฐานที่เป็นประโยชน์แก่เจ้าของข้อมูลหรือให้ภาระการพิสูจน์ตกแก่ฝ่ายผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลไว้โดยเฉพาะ”
- ในขณะที่ ผู้ช่วยผู้อำนวยการฝ่ายบริหารความเสี่ยงภาพรวมของธนาคารแห่งประเทศไทย ซึ่งอยู่ในคณะทำงานคุ้มครองข้อมูลส่วนบุคคลขององค์กร มีความเห็นว่า “DPO เป็นคนกลางระหว่างเจ้าของข้อมูลกับสถาบันการเงิน ซึ่งมีหน้าที่ต้องติดตามและคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องตามที่กฎหมายกำหนด รวมทั้งเป็นผู้มีความเข้าใจถึงการใช้งานข้อมูลส่วนบุคคลขององค์กรดีอยู่แล้ว จึงไม่มีความ

[156] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

จำเป็นต้องตัดพยาน ส่วนคำให้การของ DPO ในฐานะพยานนั้นจะรับฟังได้มากน้อยเพียงใดเป็นหน้าที่ในการชั่งน้ำหนักพยานหลักฐานของศาล”[157]

ในขณะที่ DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “หากเป็นกรณีคดีละเมิดข้อมูลส่วนบุคคล DPO ไม่ควรเป็นตัวแทนหรือเป็นพยานขององค์กรในการพิจารณาคดี เพราะ DPO อาจเลือกที่จะไม่ให้ข้อมูลหรือความเห็น อันทำให้เกิดความขัดแย้งทางผลประโยชน์ได้”[158]

หากมีประเด็นข้อพิพาทเรื่องการคุ้มครองข้อมูลส่วนบุคคล ผู้เขียนมีความเห็นว่าไม่ควรมีกฎหมายกำหนดห้ามมิให้ DPO เป็นตัวแทนหรือพยานในการพิจารณาคดีของศาล หรือห้ามมิให้เป็นผู้ชี้แจ้งข้อเท็จจริงในกรณีที่เจ้าข้อมูลส่วนบุคคลร้องเรียนการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ของสถาบันการเงินต่อคณะกรรมการผู้เชี่ยวชาญตามมาตรา 73 เพราะโดยทั่วไป DPO เป็นบุคคลหนึ่งที่มีความเข้าใจการจัดเก็บและการประมวลผลข้อมูลส่วนบุคคลภายในสถาบันการเงินที่ได้รับการแต่งตั้งเป็นอย่างดี หากมีโครงสร้างองค์กรที่มีความเป็นอิสระและปราศจากความขัดแย้งทางผลประโยชน์ ย่อมไม่มีความจำเป็นในการห้ามตามลักษณะดังกล่าว ในแง่ของเจ้าของข้อมูลนั้น ไม่ว่ากฎหมายเรื่องเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะมีเจตนารมณ์ในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม เจ้าของข้อมูลสามารถขอคำแนะนำจากที่ปรึกษากฎหมาย หรือว่าจ้างทนายความเพื่อช่วยรวบรวมพยานหลักฐานในการดำเนินคดีได้อยู่แล้ว ทั้งนี้ ข้อที่ว่า DPO ของสถาบันการเงินจะเบิกความหรือให้การเท็จหรือไม่น่าจะไม่ใช่ประเด็นปัญหา เพราะการรับฟังและชั่งน้ำหนักพยานหลักฐานเป็นหน้าที่ของศาล

3.5 ระยะเวลาและการพ้นจากตำแหน่งของ DPO

การแต่งตั้ง DPO ที่มีกำหนดระยะเวลาการปฏิบัติหน้าที่ไว้แน่นอน (permanent/ undetermined contract)[159] รวมถึงกำหนดเงื่อนไขของการพ้นจากตำแหน่งก่อนครบกำหนดระยะเวลาดังกล่าวล้วนเป็นปัจจัยสำคัญอย่างหนึ่งอันส่งผลต่อการรับรองความเป็นอิสระ ยิ่งบุคคลที่

[157] วีระ ประเสริฐนุกูล, เรื่องเดิม

[158] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[159] Network of Data Protection Officers of the EU institution and bodies. Ibid.

เป็น DPO สามารถกำหนดระยะเวลาปฏิบัติหน้าที่ได้นานมากเท่าใด จะเป็นสิ่งที่สนับสนุนให้ DPO สามารถปฏิบัติหน้าที่และตัดสินใจได้อย่างอิสระ[160]

ในหัวข้อนี้ผู้เขียนได้ทำการศึกษาวิจัยจากบทบัญญัติแห่งกฎหมาย และแนวปฏิบัติที่เกี่ยวข้องกับระยะเวลาและการพ้นจากตำแหน่งของ DPO รวมถึงวิธีการให้คุ้มครองตำแหน่งการปฏิบัติงานของ DPO (employment status) ซึ่งมีความสัมพันธ์กับความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO ดังที่ผู้เขียนได้กล่าวถึงไว้แล้วใน “หัวข้อ 3.3 ความเป็นอิสระ” โดยแบ่งประเด็นที่ทำการศึกษาวิจัยออกเป็น 3 ประเด็นย่อย ได้แก่ (1) ระยะเวลาการปฏิบัติหน้าที่ของ DPO (2) การคุ้มครองตำแหน่งการปฏิบัติงานของ DPO ตามคำสั่งแต่งตั้งของสถาบันการเงิน และ (3) การคุ้มครองตำแหน่ง DPO จากหน่วยงานกำกับดูแล

3.5.1 ระยะเวลาการปฏิบัติหน้าที่

เมื่อ DPO มีความจำเป็นจะต้องเข้าใจกิจกรรมการประมวลผลทั้งหมดของสถาบันการเงินอย่างถ่องจริง เพื่อสามารถให้คำปรึกษาและคำแนะนำอย่างเหมาะสม สถาบันการเงินควรจัดจ้าง DPO เป็นระยะเวลายาวที่สุดเท่าที่จะทำได้ หรืออย่างน้อยเป็นระยะเวลาห้าปี และเมื่อพ้นจากวาระอาจได้รับการแต่งตั้งให้กลับเข้าปฏิบัติหน้าที่เป็น DPO ได้อีก (reappointment)[161] โดยควรกำหนดเงื่อนไขของการเข้ารับให้ดำรงตำแหน่งเดิมตามความเหมาะสม[162] รวมถึงเพดานระยะเวลาสูงสุด

---

[160] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.12.

[161] ผู้เขียนเรียบเรียงจาก EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.12. และ Network of Data Protection Officers of the EU institution and bodies, Professional Standards for Data Protection Officers of the EU institution and bodies working under Regulation (EC) 45/2001 (2010). p.7.

[162] EDPS, "Position of the DPO in the organigramme," [Online] Accessed: 17 Jan 2021. Available from: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (แต่ละองค์กรมีหน้าที่กำหนดระยะเวลาในการปฏิบัติหน้าที่และเงื่อนไขในการพ้นจากตำแหน่งของ DPO สำหรับระยะการปฏิบัติหน้าที่ของ DPO ขององค์กรในสหภาพยุโรปคือตั้งแต่ 3-5 ปี และอาจได้รับการแต่งตั้งให้กลับเข้าปฏิบัติหน้าที่ได้อีกต่อเมื่อได้รับความเห็นชอบจาก EDPS ซึ่งเป็นหน่วยงานกำกับดูแล)

สถาบันการเงินไม่ควรเปลี่ยน DPO บ่อยครั้งเพราะ อาจทำให้เกิดการเสียเวลาในการเรียนรู้ของ DPO คนใหม่ และทำให้การดำเนินงานขององค์กรหยุดชะยัก ไม่ต่อเนื่อง หรือล่าช้าไปได้

ในการดำเนินการศึกษาวิจัยเรื่องระยะเวลาการปฏิบัติหน้าที่ของ DPO ซึ่งมีความสัมพันธ์กับความเป็นอิสระในการปฏิบัติงาน ผู้เขียนได้สัมภาษณ์ DPO ของแต่ละสถาบันการเงินรวม 13 แห่ง โดยมีคำถามที่ใช้ในการสัมภาษณ์ ดังนี้

- ตามสัญญาการทำงานของ DPO มีการกำหนดระยะเวลาการดำรงตำแหน่งไว้แน่นอนหรือไม่ ถ้ามี กำหนดไว้นานเพียงใด
- ท่านเห็นด้วยหรือไม่ หากมีกฎหมายกำหนดระยะเวลาดำรงตำแหน่งของ DPO ไว้แน่นอน หากเห็นด้วย ควรกำหนดไว้นานเท่าใด

ตารางที่ 27 ระยะเวลาการปฏิบัติหน้าที่ DPO ในการแต่งตั้งของสถาบันการเงิน

กำหนดระยะเวลาการปฏิบัติหน้าที่ DPO ในสถาบันการเงิน	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ไม่มีกำหนดวาระการปฏิบัติหน้าที่ DPO	5	1	6
ไม่มีกำหนดวาระการปฏิบัติหน้าที่ DPO แต่มีการทบทวนการทำงานของ DPO เป็นประจำ	-	1	-

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ผลการสัมภาษณ์พบว่า[163] ปัจจุบันการแต่งตั้ง DPO ของสถาบันการเงินทั้ง 13 แห่ง เป็นการแต่งตั้งโดยคำสั่งแต่งตั้งของผู้บริหารระดับสูงหรือคณะกรรมการของสถาบันการเงินให้พนักงานประจำภายในสถาบันการเงินแต่ละแห่ง (in-house) ทำหน้าที่เป็น DPO ตามมาตรา 41 และมาตรา 42 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ จึงไม่มีการกำหนดเพดานสูงสุดของระยะเวลาการปฏิบัติหน้าที่ไว้แน่นอนว่าห้ามเกินระยะเวลาเท่าใด อย่างไรก็ดี ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “ถึงแม้ไม่มีกำหนดวาระการดำรงตำแหน่ง แต่องค์กรได้จัดให้มีการทบทวนปฏิบัติงานของ DPO เป็นระยะๆ เช่น 6 เดือนหรือ 1 ปีตามความเหมาะสม” ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งเสริมว่า “แม้จะไม่มีกำหนดวาระการดำรงตำแหน่ง แต่ต้องมีการทบทวนการปฏิบัติงานของ DPO ปีละ 1 ครั้ง เช่นเดียวกับกระบวนการประเมินผลการทำงานรายปีของพนักงานทั่วไปของสถาบันการเงิน”

[163] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 28 ความเห็นของผู้ให้สัมภาษณ์กรณีมีกฎหมายกำหนดระยะเวลาการปฏิบัติหน้าที่ DPO ในสถาบันการเงิน

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ไม่มีความจำเป็นในการกำหนดระยะเวลา	5	2	3
เห็นว่ามีความจำเป็นต้องกำหนดระยะเวลา	-	-	3
ความเห็นของสคส.[164] สถาบันการเงินแต่ละแห่งอาจกำหนดไว้ก็ได้ขึ้นอยู่กับการบริหารจัดการภายใน เช่น หากมีข้อกังวลว่าข้อมูลความลับจะรั่วไหล หรืออาจทำให้ DPO รู้จักลูกค้ามากเกินไป			

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ผู้เขียนได้สอบถามบุคคลดังกล่าวต่อไปว่า DPO เป็นตำแหน่งที่กฎหมายมีความจำเป็นต้องกำหนดระยะเวลาการปฏิบัติหน้าที่ของ DPO ไว้แน่นอนหรือไม่

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์จากสถาบันการเงิน 10 แห่ง (สถาบันการเงินขนาดใหญ่ 5 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 3 แห่ง) ที่ไม่เห็นด้วยกับการกำหนดระยะเวลาการปฏิบัติหน้าที่ของ DPO ได้ให้เหตุผลที่สำคัญไว้ดังต่อไปนี้[165]

- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “หากสามารถปฏิบัติงานในฐานะเป็น 2nd line ได้อย่างเหมาะสม DPO จะไม่มีอำนาจตัดสินใจในผลประโยชน์ของการทำธุรกิจ ไม่ใช่ตำแหน่งที่อาจนำไปสู่การใช้อำนาจโดยไม่ชอบ” ซึ่งสอดคล้องกับที่ผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งกล่าวไว้ดังนี้ “...แตกต่างจากกรรมการของสถาบันการเงินซึ่งมีอำนาจตัดสินใจและมีส่วนได้เสียในผลประโยชน์ของการทำธุรกิจสถาบันการเงิน จึงไม่จำเป็นต้องกำหนดวาระการดำรงตำแหน่ง DPO ไว้”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “เนื่องจากบุคคลที่ดำรงตำแหน่ง DPO ต้องมีความรู้ความเข้าใจกฎหมายและต้องมีประสบการณ์การทำงานกับธนาคาร การแต่งตั้งพนักงานคนใหม่เป็น DPO บุคคลนั้นจะใช้เวลานานในการเรียนรู้รูปแบบธุรกิจและการประมวลของธนาคารฯ ซึ่งอาจทำให้การปฏิบัติงานขาดความต่อเนื่องได้”
- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “ระยะเวลาการดำรงตำแหน่งควรขึ้นอยู่กับบริบทของแต่ละองค์กร และประสิทธิภาพในการปฏิบัติงานของ DPO เป็น

[164] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[165] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

สำคัญ แต่ควรมีการประเมินอย่างใกล้ชิดและมีรอบการประเมินที่แน่นอน เช่น 6 เดือน หรือ 1 ปี”

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “การกำหนดระยะเวลาไว้ตายตัวอาจจะมีปัญหาในการสรรหา DPO ซึ่งอาจไม่ได้มีบุคลากรที่มีความรู้ความเชี่ยวชาญในองค์กรเป็นจำนวนมาก หากมีการเปลี่ยนแปลง DPO บ่อยครั้ง เช่น ทุก 2-3 ปี จะทำให้ DPO ขาดความเชี่ยวชาญในการทำงานกับสถาบันการเงินแห่งนั้น รวมถึงอาจไม่มีงบประมาณเพียงพอในการไปว่าจ้างบุคคลภายนอกมาเป็น DPO”
- ผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “ไม่มีความจำเป็นต้องกำหนดไว้ เพราะระยะเวลาการดำรงตำแหน่งของไม่เกี่ยวข้องกับความเป็นอิสระของ DPO หากสถาบันการเงินมีรูปแบบวัฒนธรรมในการบริหาร มีสายบังคับบัญชา และสายการตรวจสอบที่ดีย่อมทำให้ DPO สามารถปฏิบัติหน้าที่ได้อย่างอิสระ”

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดเล็ก 3 แห่ง ที่เห็นว่าควรมีการกำหนดระยะเวลาการปฏิบัติหน้าที่ของ DPO มีความเห็นที่สำคัญดังนี้[166]

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “DPO เป็นอาชีพที่มีเงินเดือนสูงและจำเป็นต้องสอบได้ใบรับรองคุณวุฒิ (Certification) หากให้ DPO ดำรงตำแหน่งได้อย่างไม่มีกำหนดเวลาอาจทำให้เกิดความหละหลวมในการปฏิบัติหน้าที่ตามกฎหมาย นอกจากนี้เมื่อผู้ดำรงตำแหน่ง DPO จนครบวาระก็สามารถไปทำงานด้านอื่นในองค์กรหรืออาจย้ายไปเป็น DPO ขององค์กรแห่งอื่นก็ได้ จึงควรกำหนดระยะเวลาการปฏิบัติหน้าที่ไว้ให้ชัดเจน เช่น DPO สามารถดำรงตำแหน่งได้ไม่เกินคราวละ 4 ปีและดำรงตำแหน่งติดต่อกันได้ไม่เกิน 8 ปี”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “ควรมีการทบทวนตำแหน่ง DPO เป็นประจำ (เช่น ทุก 2 ปี) เพื่อให้ได้คำแนะนำจากแง่มุมที่หลากหลายและเพื่อเป็นการส่งเสริมศักยภาพด้านการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานขององค์กร”

[166] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

อนึ่ง ผู้ให้สัมภาษณ์รายหนึ่งซึ่งอยู่ในคณะทำงานบริกรข้อมูล (Data steward team) ของสถาบันการเงินแห่งขนาดเล็กหนึ่งเห็นว่าควรแยกพิจารณาออกเป็นสองกรณี กรณีแรกคือสถาบันการเงินแต่งตั้งพนักงานภายในองค์กรเป็น DPO และกรณีที่สองคือสถาบันการเงินแต่งตั้งให้บุคคลภายนอกเป็น DPO ดังที่กล่าวว่า “ในกรณีที่สถาบันการเงินแต่งตั้งบุคคลภายในองค์กรเป็น DPO ระยะเวลาในการปฏิบัติหน้าที่ควรขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร จึงไม่ควรมีกฎหมายจะกำหนดระยะเวลาดำรงตำแหน่งของ DPO ไว้ตายตัว ส่วนกรณีที่สถาบันการเงินแต่งตั้งบุคคลภายนอกองค์กรเป็น DPO (DPO Service) ควรจำกัดระยะเวลาดำรงตำแหน่งให้อย่างชัดเจน”

ในประเด็นดังกล่าว เจ้าหน้าที่จาก สคส. ท่านหนึ่งมีความเห็นว่า[167] “สถาบันการเงินแต่ละแห่งอาจกำหนดไว้ก็ได้ขึ้นอยู่กับการบริหารจัดการภายใน เช่น หากมีข้อกังวลว่าข้อมูลความลับจะรั่วไหล หรืออาจทำให้ DPO รู้จักลูกค้ามากเกินไป”

3.5.2 การคุ้มครองตำแหน่งการปฏิบัติงานตามคำสั่งแต่งตั้งของสถาบันการเงิน

มาตรการอีกประการหนึ่งที่แสดงถึงความสำคัญของความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO คือ การคุ้มครองตำแหน่งการปฏิบัติงานของ DPO (protected employment status) ดังจะเห็นได้จากการที่กฎหมายกำหนดว่า “ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้ DPO ออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้”[168] อย่างไรก็ดี บทบัญญัติเกี่ยวกับการคุ้มครอง DPO ตามกฎหมายไทยดังกล่าวมีความแตกต่างจาก GDPR บางประการ กล่าวคือ ตาม GDPR กฎหมายป้องกันมิให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลให้ DPO ออกจากงานหรือเลิกสัญญาการจ้าง รวมถึงไม่สามารถลงโทษ (penalise) ด้วยวิธีอื่นใดด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตามกฎหมายได้[169]

---

[167] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[168] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 วรรค 3 และตามมาตรา 82 การให้ DPO ออกจากงานหรือเลิกจ้างเพราะเหตุที่ปฏิบัติตามกฎหมายนั้น อันเป็นการฝ่าฝืนพระราชบัญญัติฯ ต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท

[169] GDPR, Article 38(3)

คำว่า “ลงโทษ” ตาม GDPR, Article 38(3) นั้น EDPS ตีความว่ารวมถึงการที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกำหนดบทลงโทษอื่นใด (penalty) ด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น การปฏิเสธไม่ให้สิทธิประโยชน์ที่เขาพึงได้รับ (denial of benefits) การไม่ให้เลื่อนตำแหน่ง (delay of promotion) หรือการกำหนดมาตรการอันเป็นการเลือกปฏิบัติ (discriminatory measure)[170]

ข้อพิจารณาที่สำคัญอีกประการหนึ่ง คือ กฎหมายกำหนดห้ามมิให้ลงโทษ DPO ด้วยเหตุที่เขาปฏิบัติหน้าที่หรือภารกิจตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น (for performing tasks) เช่น หาก DPO พิจารณาแล้วเห็นว่าการประมวลผลข้อมูลส่วนบุคคลของของสถาบันการเงินแห่งหนึ่งมีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของเจ้าของข้อมูล และได้แจ้งให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลทราบแล้วแต่กรณีทราบแล้ว แต่บุคคลดังกล่าวรวมถึงฝ่ายบริหารจัดการความเสี่ยงขององค์กรไม่เห็นด้วยกับการประเมินของ DPO ในกรณีนี้สถาบันการเงินไม่อาจให้ DPO ออกจากการปฏิบัติหน้าที่หรือลงโทษได้ เนื่องจาก DPO มีหน้าที่ในการให้คำแนะนำการประเมินความเสี่ยงของผลกระทบการคุ้มครองข้อมูลส่วนบุคคล

ในการสนับสนุนให้เกิดแนวปฏิบัติอันแบบอย่างที่ดีและเพื่อสร้างความตระหนักแก่คณะกรรมการผู้บริหารว่ามีการรับรองความเป็นอิสระในการปฏิบัติงานของ DPO สถาบันการเงินควรกำหนดไว้ในสัญญาว่าจ้างหรือหนังสือแต่งตั้ง DPO ให้ชัดเจนว่าบุคคลที่ได้รับแต่งตั้งนั้นจะไม่ถูกให้ออกจากงาน หรือเลิกสัญญา หรือถูกลงโทษอย่างใดอย่างหนึ่งด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ และกฎหมายอื่นที่เกี่ยวข้อง[171]

ด้วยเหตุนี้ ผู้เขียนจึงทำการสัมภาษณ์ DPO และผู้ปฏิบัติงานที่เกี่ยวข้องของแต่ละสถาบันการเงินว่า ในการแต่งตั้งมีการรับรองว่า DPO จะไม่ถูกให้ออกจากงาน หรือเลิกสัญญา หรือถูกลงโทษ

---

[170] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.10.

[171] การให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเพราะเหตุที่ปฏิบัติตามกฎหมายนั้นเป็นการฝ่าฝืนมาตรา 82 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

ใดๆ จากการปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไว้เป็นลายลักษณ์อักษรอย่างชัดเจนหรือไม่ หากไม่ เพราะเหตุใด

ตารางที่ 29 การกำหนดคุ้มครองตำแหน่ง DPO ในสถาบันการเงินตามมาตรา 42 วรรคสาม

การคุ้มครองตำแหน่งการปฏิบัติงานของ DPO	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ไม่มีการกำหนดไว้	5	2	5
มีการกำหนดไว้ในเอกสารแต่งตั้ง	-	-	1
ข้อเสนอแนะเพิ่มเติมของผู้ให้สัมภาษณ์ - เช่นเดียวกับผู้ปฏิบัติหน้าที่ในฐานะ 2nd Line ทั่วไป DPO ควรจะได้รับการดูแลจากหน่วยงานกำกับดูแล หากเกิดกรณีเปลี่ยน ย้าย ตัดเงินเดือน หรือลงโทษอื่นๆ ที่ส่งผลกระทบต่อ DPO นั้นสถาบันการเงินต้องรายงานหรือขออนุญาตจากหน่วยงานกำกับดูแล - ก่อนดำเนินการลงโทษ สถาบันการเงินควรตั้งคณะกรรมการสอบสวนข้อเท็จจริง โดยต้องไม่มีผู้บริหารองค์กรอยู่ในคณะกรรมการดังกล่าว			

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[172] ในทางปฏิบัติคำสั่งแต่งตั้ง DPO ของสถาบันการเงินส่วนใหญ่ (12 แห่ง) จะมิได้ให้การคุ้มครองตำแหน่งว่า DPO จะไม่ถูกให้ออกจากงาน หรือเลิกสัญญา หรือถูกลงโทษใดๆ จากการปฏิบัติหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งผู้ให้สัมภาษณ์ของสถาบันการเงินดังกล่าวมีความเห็นไปในแนวทางเดียวกันว่า เนื่องจาก DPO ย่อมได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และและกฎหมายแรงงานที่เกี่ยวข้องอยู่แล้ว และผู้บริหารของสถาบันการเงินแต่ละแห่งต่างทราบข้อกฎหมายเรื่องดังกล่าวเป็นอย่างดี จึงไม่จำเป็นต้องกำหนด

ในขณะที่ สถาบันการเงินขนาดเล็กเพียง 1 แห่งได้กำหนดการคุ้มครองตำแหน่งการปฏิบัติงานของ DPO ไว้ในเอกสารแต่งตั้งอย่างชัดเจน โดยมีใจความสำคัญว่า “การแต่งตั้ง DPO ของสถาบันการเงินนั้นแยกต่างหากและไม่มีผลต่อความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง (employment relationship) และสถาบันการเงินจะไม่ให้ DPO ออกจากการปฏิบัติหน้าที่ หรือเลิกสัญญาที่ทำขึ้น ด้วยเหตุที่ DPO ปฏิบัติหน้าที่ตามกฎหมาย ข้อบังคับ ประกาศ หรือแนวปฏิบัติใดที่

[172] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ DPO สามารถปฏิบัติหน้าที่หรือภารกิจอื่นโดยหน้าที่หรือภารกิจนั้นจะต้องไม่ขัดแย้งกับหน้าที่ตามกฎหมายของ DPO”[173]

นอกจากนี้ ผู้ให้สัมภาษณ์มีข้อเสนอแนะเพิ่มเติมเกี่ยวกับการคุ้มครองตำแหน่งการปฏิบัติงานของ DPO บางประการ โดย DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเสนอว่า “DPO ควรจะได้รับการดูแลจากหน่วยงานกำกับดูแล เช่น หากเกิดกรณี เปลี่ยนหรือย้าย หรือ ตัดเงินเดือน หรืออื่นๆ ที่ส่งผลกระทบต่อ DPO นั้นสถาบันการเงินต้องรายงานหรือขออนุญาตจากหน่วยงานกำกับดูแล ดังเช่นที่ธนาคารแห่งประเทศไทยดำเนินการกับผู้ปฏิบัติหน้าที่ในฐานะ 2nd Line ทั่วไป” ส่วน DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งเสริมว่า “หากจะมีการลงโทษกับ DPO สถาบันการเงินควรตั้งคณะกรรมการสอบสวนข้อเท็จจริงเสียก่อน โดยไม่ควรมีบุคคลที่เป็นผู้บริหารองค์กรอยู่ในคณะกรรมการสอบสวนฯ ดังกล่าว”

3.5.3 การคุ้มครองตำแหน่ง DPO จากหน่วยงานกำกับดูแล

นอกเหนือจากเรื่องความจำเป็นในการกำหนดระยะเวลาในการปฏิบัติหน้าที่ (term of appointment) และการคุ้มครองตำแหน่งการปฏิบัติงาน (employment status) ของ DPO หน่วยงานกำกับดูแลอาจเข้ามามีบทบาทในการคุ้มครองตำแหน่ง DPO ของแต่ละองค์กร เช่น ดังที่กฎหมายของสหภาพยุโรปกำหนดว่า DPO จะถูกให้ออกจากการปฏิบัติหน้าที่ได้ต่อเมื่อบุคคลดังกล่าวไม่อยู่ในสถานะที่สามารถปฏิบัติหน้าที่ได้อีกต่อไป และจะต้องได้รับความยินยอมจากหน่วยงานกำกับดูแล[174]

ผู้เขียนได้สอบถามผู้ให้สัมภาษณ์ของสถาบันการเงินแต่ละแห่ง และผู้ให้สัมภาษณ์จากธนาคารแห่งประเทศไทย ว่าเห็นด้วยหรือไม่ หากมีการแก้ไขเพิ่มเติมกฎหมายว่า "ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะให้ DPO ออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่ปฏิบัติหน้าที่ตามกฎหมายไม่ได้ เว้นแต่บุคคลดังกล่าวไม่อยู่ในสถานะที่สามารถปฏิบัติหน้าที่ได้อีกต่อไปและการพ้นจากตำแหน่งของ DPO ต้องได้รับอนุญาตจากหน่วยงานกำกับดูแล"

---

[173] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[174] Regulation (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Article 44(8)

ในเบื้องต้นผลการสัมภาษณ์พบว่า[175] เมื่อสถาบันการเงินทำการแต่งตั้งหรือปลด DPO ออกจากการปฏิบัติหน้าที่ สถาบันการเงินต่างๆ เห็นด้วยว่ามีหน้าที่แจ้งการแต่งตั้งและการปลดจากตำแหน่ง DPO ต่อหน่วยงานกำกับดูแล เช่น ธนาคารแห่งประเทศไทย หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้หน่วยงานกำกับดูแลติดต่อประสานงานกับ DPO อย่างถูกต้อง

ตารางที่ 30 ความเห็นของผู้ให้สัมภาษณ์ เรื่อง การแต่งตั้งและการพ้นจากตำแหน่ง DPO ต้องขออนุญาตจากหน่วยงานกำกับดูแลหรือไม่

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ควรได้รับอนุญาตจากหน่วยงานกำกับดูแล	1	-	3
ไม่เห็นด้วยกับการขออนุญาตจากหน่วยงานกำกับดูแล	4	2	3
ความเห็นของสคส.[176] การแต่งตั้งและการพ้นจากตำแหน่ง DPO ควรขึ้นอยู่กับการบริหารจัดการภายในของแต่ละสถาบันการเงิน และชี้ว่าปัจจุบัน สคส. ซึ่งเป็นหน่วยงานกำกับดูแลเพียงแห่งเดียวยังไม่มีความพร้อมในการกำกับดูแล DPO ของทุกองค์กรในประเทศได้อย่างครอบคลุม			

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ผู้ให้สัมภาษณ์จากสถาบันการเงิน 4 แห่ง (ขนาดใหญ่ 1 แห่ง และขนาดเล็ก 3 แห่ง) เห็นด้วยว่าการแต่งตั้งหรือการพ้นจากตำแหน่งของ DPO ควรได้รับอนุญาตจากหน่วยงานกำกับดูแล โดยมีเหตุผลที่สำคัญดังนี้[177]

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “การปฏิบัติหน้าที่ในฐานะ DPO ควรได้รับการดูแลจากหน่วยงานกำกับดูแล เช่น หากเกิดกรณี เปลี่ยนหรือย้าย หรือ ตัดเงินเดือนหรืออื่นๆ ที่ส่งผลกระทบต่อ DPO จะต้องรายงานหรือขออนุญาตจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกับที่ธนาคารแห่งประเทศไทยดำเนินการกับผู้ปฏิบัติงาน 2nd Line ทั่วไป”
- ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง เห็นว่า “การปฏิบัติงานของ DPO ในภาคเอกชนมีความเป็นไปได้ที่อาจเกิดการขัดแย้งต่อผลประโยชน์ขององค์กร ซึ่งในทางปฏิบัติผู้บริหารระดับสูงของสถาบันการเงินเอกชนอาจกดดันหรือลงโทษทางวินัย

[175] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[176] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[177] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

จนทำให้ DPO ที่มีความคิดเห็นแตกต่างและขัดกับผลประโยชน์ขององค์กรต้องออกจากตำแหน่ง ดังนั้น กฎหมายอาจกำหนดกลไกบางประการ เช่น สถาบันการเงินแต่ละแห่งมีหน้าที่ต้องส่งคุณสมบัติและลักษณะต้องห้ามของ DPO ให้หน่วยงานกำกับดูแลพิจารณาเพิ่มเติม”

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “DPO จำเป็นต้องมีการลงทะเบียนกับหน่วยงานกำกับดูแล เพื่อให้หน่วยงานกำกับดูแลติดตามข้อมูลการปฏิบัติงานและประสานงานกับ DPO ของแต่ละสถาบันการเงินได้ง่าย และไม่ใช่เรื่องยากที่ก่อให้เกิดภาระเกินสมควรต่อสถาบันการเงิน”
- DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งเห็นว่า “เป็นการทำให้หน่วยงานกำกับดูแลเป็นผู้คุ้มครองตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอีกชั้นหนึ่ง อาจมีกฎหมายกำหนดให้บุคคลที่จะปฏิบัติหน้าที่เป็น DPO ต้องสอบได้ใบอนุญาต และไม่ได้มองว่าเป็นภาระ”

ในขณะที่ผู้ให้สัมภาษณ์จากสถาบันการเงิน 9 แห่ง (ขนาดใหญ่ 4 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 3 แห่ง) ไม่เห็นด้วยกับการขออนุญาตในการแต่งตั้งหรือการพ้นจากตำแหน่ง DPO ของสถาบันการเงิน และมีความเห็นที่สำคัญว่า[178]

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “การแต่งตั้งและการปลดจากตำแหน่งของ DPO ควรเป็นกระบวนการพิจารณาภายในของแต่ละสถาบันการเงิน โดย DPO ที่ถูกให้ออกจากงานหรือถูกลงโทษอย่างอื่นสามารถใช้สิทธิอุทธรณ์ตามกระบวนการของกฎหมายแรงงานได้อยู่แล้ว ไม่ควรต้องขออนุญาตจากหน่วยงานกำกับดูแล แต่อาจมีการกำหนดให้หน่วยงานกำกับดูแลเป็นผู้พิจารณาอนุมัติหรือเพิกถอนใบอนุญาตอาชีพ DPO ก็ได้” DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งเสริมว่า “สถาบันการเงินแต่ละแห่งควรเป็นผู้พิจารณาคัดเลือกและพิจารณาการพ้นจากตำแหน่งของ DPO เพื่อให้องค์กรเกิดการพัฒนาได้อย่างยั่งยืนด้วยตนเอง”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “ไม่มีความจำเป็นต้องมีกฎหมายกำหนดให้ขออนุญาตจากหน่วยงานกำกับดูแล เพราะการแต่งตั้งบุคลากรระดับผู้บริหาร

[178] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ของสถาบันการเงินต้องรายงานให้ธนาคารแห่งประเทศไทยทราบตามกระบวนการกฎหมาย ประกอบกับสถาบันการเงินมีกระบวนการ Check and Balance ที่เพียงพอและต้องติดต่อประสานงานกับ ธปท. เป็นประจำอยู่แล้ว”

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “หากองค์กรได้ออกแบบโครงสร้างของ DPO ให้มีความอิสระอยู่แล้วจึงไม่จำเป็นต้องขออนุญาตจากหน่วยงานกำกับดูแล”
- เจ้าหน้าที่อาวุโสฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่งมีความเห็นว่า “การนำระบบลงทะเบียนหรือระบบขออนุญาตมาใช้กับตำแหน่ง DPO ของภาคสถาบันการเงินก่อให้เกิดภาระแก่องค์กรโดยไม่จำเป็น เนื่องจากมีค่าอบรมวิชาชีพที่เพิ่มขึ้น อีกทั้งระบบงานและวิธีการจัดการงานด้านข้อมูลส่วนบุคคลของแต่ละสถาบันการเงินมีความแตกต่างกัน”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “การที่จะต้องไปขออนุญาตกับหน่วยงานกำกับดูแลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จะเพิ่มภาระหน้าที่ให้แก่ทั้งสองหน่วยงานอย่างมาก ซึ่งไม่แน่ใจว่ามีความพร้อมในการรองรับการดำเนินการหรือไม่”

อนึ่ง เจ้าหน้าที่ของสคส. ท่านหนึ่ง กล่าวว่า[179] “การแต่งตั้งและการพ้นจากตำแหน่งควรขึ้นอยู่กับการบริหารจัดการภายในของแต่ละสถาบันการเงิน ไม่ควรต้องขอความเห็นชอบจากหน่วยงานกำกับดูแล” และชี้ว่าเนื่องจากเป็นหน่วยงานกำกับดูแลเพียงแห่งเดียวในปัจจุบัน ทางสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังไม่มีความพร้อมมากเพียงพอที่จะกำกับดูแล DPO ของทุกองค์กรในประเทศไทยได้อย่างครอบคลุม

ในประเด็นดังกล่าว จะเห็นได้ว่าผู้ให้สัมภาษณ์ที่เห็นด้วยกับการที่จะมีกฎหมายกำหนดให้สถาบันการเงินต้องขออนุญาตจากหน่วยงานกำกับดูแลก่อนการปลด DPO ออกจากการปฏิบัติหน้าที่ส่วนใหญ่เป็นผู้ให้สัมภาษณ์จากสถาบันการเงินขนาดเล็กที่ไม่มีการติดต่อสัมพันธ์กับธนาคารแห่งประเทศไทยอย่างใกล้ชิด จึงต้องการให้มีหน่วยงานกำกับดูแลเข้ามารับรองความเป็นอิสระและคุ้มครองตำแหน่งหน้าที่ DPO เพิ่มเติม ในทางตรงข้ามสถาบันการเงินที่ไม่เห็นด้วยนั้น ผู้เขียนมี

[179] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

ความเห็นว่าเป็นสถาบันการเงินที่มีโครงสร้างจัดการความเป็นอิสระที่ดีและมีอยู่ภายใต้การกำกับดูแลของ ธปท. อย่างใกล้ชิดอยู่แล้ว จึงไม่มีความจำเป็นต้องมีกฎเกณฑ์ในลักษณะดังกล่าวอีก

ทั้งนี้ ปัจจุบันมีกฎหมายที่กำหนดให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับหลักดูแลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เข้ามามีส่วนเกี่ยวข้องในการกำกับดูแลการแต่งตั้ง การถอนหรือการเปลี่ยนแปลง DPO ของแต่ละองค์กร โดยกำหนดว่า “เมื่อ สคส. ได้รับแจ้งการแต่งตั้ง DPO แล้ว ให้สำนักงานฯ ตรวจสอบเอกสารและหลักฐาน หากเอกสารและหลักฐานครบถ้วนถูกต้องตามกรณี ให้สำนักงานฯ รับแจ้ง แต่หากเอกสารหรือหลักฐานไม่ครบถ้วนถูกต้องให้แจ้งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแก้ไขเพิ่มเติมภายในเวลาอันสมควร การถอนหรือเปลี่ยนแปลงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งแก่สำนักงานและเจ้าของข้อมูลส่วนบุคคลทราบไม่เกิน 10 วัน นับแต่มีการเพิกถอนหรือเปลี่ยนแปลงตามพร้อมแนบหลักฐานที่เกี่ยวข้อง”[180]

3.6 ผู้ช่วย DPO และผู้แทน DPO

ในการดำเนินธุรกิจและการดำเนินกระบวนการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล แต่ละองค์กรอาจแต่งตั้งผู้ช่วย DPO (Assistant DPO) หรือผู้แทน DPO (Acting DPO) เพื่อทำหน้าที่ให้ความช่วยเหลือและรับรองความต่อเนื่องของการปฏิบัติหน้าที่ตามกฎหมายในกรณีที่ DPO ไม่สามารถปฏิบัติงานได้ EDPS มีความเห็นว่า[181] ถึงแม้จะไม่มีกฎหมายกำหนดประเด็นเกี่ยวกับสถานะของผู้ช่วยหรือผู้แทน DPO ไว้ก็ตาม ควรมีการบัญญัติรับรองสถานะบุคคลดังกล่าวเช่นเดียวกับการรับรองสถานะความเป็นอิสระและปราศจากความขัดแย้งทางผลประโยชน์ของ DPO

ด้วยเหตุนี้ ผู้เขียนจึงได้ทำการสัมภาษณ์สถาบันการเงินต่างๆ ว่ามีการแต่งตั้งผู้ช่วย DPO (Assistant DPO) หรือผู้แทน DPO (Acting DPO) หรือไม่ พบว่า เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ไม่ได้กำหนดให้องค์กรมีหน้าที่แต่งตั้งผู้ช่วยหรือผู้แทน DPO จึงมีทั้งสถาบันการเงิน

---

[180] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.10. โปรดดู https://www.law.chula.ac.th/event/10941/

[181] EDPS. Position paper on the role of Data Protection Officers of the EU institutions and bodies. Ibid, p.10.

ที่แต่งตั้งและสถาบันการเงินที่มิได้แต่งตั้ง โดยสถาบันการเงินที่มีการแต่งตั้งผู้ช่วยหรือผู้แทน DPO มีจำนวนใกล้เคียงกับสถาบันการเงินที่ไม่มีการแต่งตั้งบุคคลดังกล่าว

ตารางที่ 31 การแต่งตั้งผู้ช่วยหรือผู้แทน DPO (Assistant or Acting DPO) ของสถาบันการเงินผู้ให้สัมภาษณ์

ผู้ช่วย/ผู้แทน DPO	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
แต่งตั้งแล้ว	4	1	1
ยังไม่มีการแต่งตั้ง (แต่มีผู้ประสานงาน)	1	1	5

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[182] สถาบันการเงิน 6 แห่ง ได้มีการแต่งตั้งผู้ช่วยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ซึ่งจำนวนผู้ช่วยหรือผู้แทน DPO ของสถาบันการเงินแต่ละแห่งที่มีการแต่งตั้งบุคคลดังกล่าวมีความแตกต่างกันตามขนาดของสถาบันการเงิน สถาบันการเงินขนาดใหญ่และขนาดกลางจะมีจำนวนผู้ช่วยหรือผู้แทน DPO ประมาณ 10-20 คน ในขณะที่สถาบันการเงินขนาดเล็กจะมีจำนวนผู้ช่วยหรือผู้แทน DPO ประมาณ 2-5 คน) ส่วนสถาบันการเงินอีก 7 แห่ง ไม่ได้แต่งตั้งผู้ช่วยหรือผู้แทน DPO อย่างไรก็ดีสถาบันการเงินดังกล่าวมีผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลประจำแต่ละหน่วยงานภายในองค์กร

ผู้เขียนได้สัมภาษณ์ต่อไปเกี่ยวกับการรับรองสถานะตามกฎหมายให้แก่ผู้ช่วยหรือผู้แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลว่า บุคคลดังกล่าวจำเป็นต้องมีกฎหมายรับรองความเป็นอิสระและไม่อยู่ในฐานะที่ก่อให้เกิดความขัดแย้งทางผลประโยชน์หรือไม่

ตารางที่ 32 ความเห็นของผู้ให้สัมภาษณ์ เรื่อง สถานะทางกฎหมายของผู้ช่วย DPO และผู้แทน DPO

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
ต้องรับรองสถานะของบุคคลดังกล่าวเช่นเดียวกับ DPO	4	1	5
ไม่มีความจำเป็นในการรับรองสถานะ	1	1	1

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงิน 10 แห่ง (ขนาดใหญ่ 4 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 5 แห่ง) เห็นว่าบุคคลดังกล่าวต้องสามารถปฏิบัติหน้าที่ได้อย่าง

[182] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

อิสระและไม่อยู่ในสถานะที่ก่อให้เกิดความขัดแย้งทางผลประโยชน์ เช่นเดียวกับการที่กฎหมายกำหนดรับรองสถานะของ DPO โดยมีเหตุผลที่สำคัญดังต่อไปนี้[183]

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “จำเป็นต้องมีการรับรองความเป็นอิสระและไม่มีความขัดแย้งทางผลประโยชน์ เพราะบุคคลดังกล่าวไม่ได้ปฏิบัติงานด้านข้อมูลส่วนบุคคลเพียงอย่างเดียว แต่มีความรับผิดชอบทางธุรกิจต่อสถาบันการเงินด้วย”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “ตำแหน่งผู้ช่วยหรือผู้แทน DPO ทำหน้าที่สนับสนุนการปฏิบัติหน้าที่ของ DPO ตามที่ได้รับมอบหมาย จึงมีความจำเป็นต้องมีโครงสร้างรับรองความเป็นอิสระในการปฏิบัติหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เกิดผลสัมฤทธิ์เช่นเดียวกับโครงสร้างการปฏิบัติงานของ DPO”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “จำเป็นต้องมีความเป็นอิสระ ถึงแม้ปัจจุบันกฎหมายยังไม่ได้กำหนดเกณฑ์ให้มีการแต่งตั้งผู้ช่วย DPO ขึ้นก็ตาม ในทางปฏิบัติมีความจำเป็นต้องตั้งผู้ช่วย DPO เพื่อช่วยแบ่งเบาภาระงาน อีกทั้งยังเป็นประโยชน์ในการกำหนดผู้ที่จะมาเป็น DPO ขององค์กรในอนาคต”

ผู้ให้สัมภาษณ์ของสถาบันการเงิน 3 แห่ง (ขนาดใหญ่ ขนาดกลาง และขนาดเล็กอย่างละ 1 แห่ง) ที่เห็นว่าไม่มีความจำเป็นต้องกำหนดให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ได้อย่างอิสระและไม่จำเป็นต้องอยู่ในสถานะที่ไม่มีความขัดแย้งทางผลประโยชน์ ให้เหตุผลที่สำคัญดังต่อไปนี้[184]

- เจ้าหน้าที่ฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “บุคคลในคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินสามารถทำงานร่วมกันและมีดุลพินิจในการตัดสินใจดำเนินงานให้เป็นไปตามกฎหมายอยู่แล้ว จึงไม่มีความจำเป็นต้องกำหนดการคุ้มครองดังกล่าว”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “ไม่มีความจำเป็นต้องมีการรับรองความเป็นอิสระและไม่มีความขัดแย้งทางผลประโยชน์ เนื่องจากบุคคลเป็นผู้ที่อาจมีความรับผิดชอบทางธุรกิจต่อสถาบันการเงิน”

---

[183] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[184] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งกล่าวว่า “ไม่จำเป็นต้องมีการรับรองสถานะดังกล่าว เนื่องจากต้องพิจารณาตามปริมาณงานและความจำเป็นด้านการจัดสรรทรัพยากรบุคคลของแต่ละองค์กร”

ในประเด็นข้างต้นผู้เขียนมีความเห็นว่า เนื่องจาก DPO มีหน้าที่และภารกิจงานตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดเป็นจำนวนมาก ในทางปฏิบัติสถาบันการเงินจึงไม่อาจหลีกเลี่ยงการแต่งตั้งผู้ช่วย DPO (Assistant DPO) ขึ้นเพื่อทำหน้าที่ประสานงานและสนับสนุนการปฏิบัติงานของ DPO ได้ เมื่อผู้ช่วย DPO เป็นบุคคลภายในองค์กรซึ่งมีความรับผิดชอบทั้งทางธุรกิจและการคุ้มครองข้อมูลส่วนบุคคล จึงมีต้องมีการกำหนดโครงสร้างที่รับรองสถานะความเป็นอิสระปราศจากความขัดแย้งทางผลประโยชน์ ส่วนตำแหน่งผู้แทน DPO (Acting DPO) เป็นบุคคลที่หน้าที่ความรับผิดชอบเทียบเท่า DPO อยู่แล้ว กล่าวคือถือเป็นผู้ปฏิบัติหน้าที่เป็น DPO ตามกฎหมายถึงแม้เป็นการชั่วคราวก็ตาม

บทที่ 4

ปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

สำหรับการคัดเลือกบุคคลที่จะเข้ามาทำหน้าที่เป็น DPO ของสถาบันการเงิน นอกจากการคำนึงถึงข้อพิจารณาต่างๆ เกี่ยวกับโครงสร้างการบริหารงานขององค์กรแล้ว ข้อพิจารณาอีกประการหนึ่งที่สถาบันการเงินต้องให้ความสำคัญ คือ ข้อพิจารณาด้านความสามารถของผู้ที่จะเข้ามาดำรงตำแหน่ง DPO (Competency) เนื่องจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีบทบาทหน้าที่ในการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินให้เป็นไปตามข้อบังคับของกฎหมาย และให้คำแนะนำเรื่องการคุ้มครองข้อมูลส่วนบุคคลแก่องค์กร รวมถึงอาจต้องติดต่อกับเจ้าของข้อมูลส่วนบุคคล และประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับดูแลในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 41 วรรคหก บัญญัติว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” โดยตาม GDPR และร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กำหนดเพียงหลักการทั่วไปไว้ว่า DPO ต้องสามารถปฏิบัติหน้าที่ของตนโดยคำนึงถึงความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งพิจารณาจากลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล[1] และการแต่งตั้ง DPO ต้องพิจารณาจากคุณสมบัติทางวิชาชีพ (professional quality) โดยเป็นบุคคลที่มีความเชี่ยวชาญกฎหมายและแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนความสามารถอื่นที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย[2]

จะเห็นได้ว่าปัจจุบันสภาพกฎหมายเกี่ยวกับการรับรองคุณสมบัติของ DPO ในประเทศไทยยังขาดความชัดเจน ซึ่งจากการสัมภาษณ์เจ้าหน้าที่ สคส. ท่านหนึ่งพบว่าทางคณะกรรมการคุ้มครอง

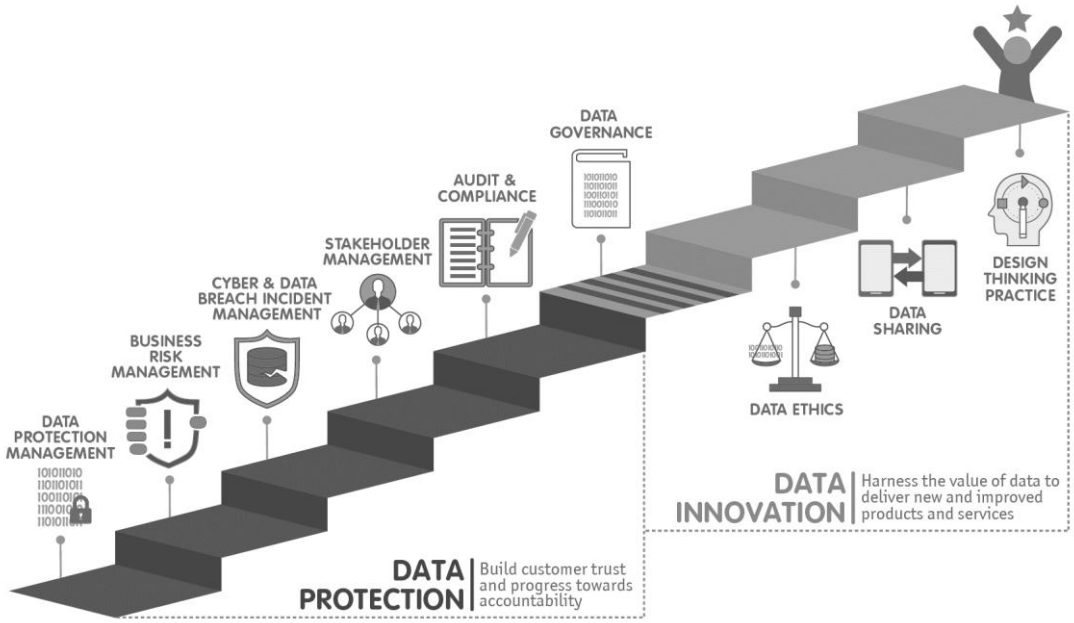
---

[1] GDPR, Article 39(2) และร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.11. โปรดดู https://www.law.chula.ac.th/event/10941/

[2] GDPR, Article 37(5)

ข้อมูลส่วนบุคคลได้วางกรอบแนวทางการพัฒนากฎหมายเกี่ยวกับความสามารถและการฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Competency Framework and Training Roadmap) โดยไม่เฉพาะเจาะจงตามอุตสาหกรรม[3] ดังภาพด้านล่างนี้

ภาพที่ 7 กรอบแนวทางการพัฒนากฎหมายเกี่ยวกับความสามารถและการฝึกอบรม DPO



ที่มา: สัมภาษณ์ ดร.สุนทรีย์ ส่งเสริม, นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 29 กรกฎาคม 2564

จากกรอบแนวทางการพัฒนากฎหมายเกี่ยวกับความสามารถและการฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลข้างต้น ตำแหน่ง DPO ควรมีทักษะ ความรู้ความเข้าใจ หรือความสามารถด้านต่างๆ ที่เกี่ยวข้องในการปฏิบัติหน้าที่ตาม เพื่อแสดงให้เห็นถึงความโปร่งใสของการประมวลผลข้อมูล (Accountability) ตลอดจนส่งเสริมมูลค่าของข้อมูลเพื่อนำมาพัฒนาผลิตภัณฑ์และการให้บริหารขององค์กร ความสามารถดังกล่าวของ DPO แบ่งออกเป็น 9 ด้าน ดังต่อไปนี้[4]

[3] ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, "สัมภาษณ์ เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล."

[4] ผู้เขียนเรียบเรียงจาก ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, เอกสารประกอบการสัมภาษณ์เรื่อง DPO Competency Framework and Training Roadmap (2564), หน้า.3-8. และ PDPC

1. การบริหารจัดหารข้อมูล (Data Protection Management) DPO ต้องมีความสามารถในการพัฒนาระบบบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมายที่เกี่ยวข้อง
2. การบริหารจัดการความเสี่ยง (Business Risk Management) DPO ต้องสามารถประเมินความเสี่ยงทางธุรกิจที่มีแนวโน้มว่าจะเกิดขึ้นได้ในปัจจุบันภายใต้ขอบเขตหน้าที่ของตน รวมถึงกำหนดแผนและมาตรการรับมือความเสี่ยงกรณีเกิดเหตุไม่คาดคิด
3. การจัดการกับเหตุการณ์ทางไซเบอร์และการรั่วไหลของข้อมูล (Cyber & Data Breach Incident Management) DPO ต้องมีความสามารถในการให้คำแนะนำเพื่อพัฒนากระบวนการจัดการกับเหตุการณ์ทางไซเบอร์และการรั่วไหลของข้อมูลขององค์กร สามารถทำความเข้าใจ วิเคราะห์เหตุการณ์ได้อย่างลึกซึ้ง และหาทางป้องกันหรือลดความเป็นไปได้ที่เหตุการณ์เหล่านั้นจะเกิดขึ้น
4. การจัดการกับผู้มีส่วนเกี่ยวข้อง (Stakeholder Management) DPO ต้องเข้ามามีส่วนร่วมและเจรจากับผู้มีส่วนเกี่ยวข้องเพื่อหาข้อสรุปที่เป็นประโยชน์กับทางสองฝ่าย เช่น ระหว่างองค์กรกับเจ้าของข้อมูล หรือระหว่างองค์กรกับหน่วยงานกำกับดูแล
5. การการตรวจสอบและกำกับการปฏิบัติตามกฎเกณฑ์ (Audit and Compliance) DPO ต้องสามารถยกระดับกระบวนการกำกับการปฏิบัติตามกฎเกณฑ์ขององค์กร โดยอาศัยการวิเคราะห์ช่องว่างทางธุรกิจและช่องว่างของกระบวนการทางเทคโนโลยีสารสนเทศ
6. การกำกับดูแลข้อมูล (Data Governance) DPO ต้องมีความสามารถในการพัฒนาแนวปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลขององค์กรครบทั้งวงจร รวมถึงเข้าใจการแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างองค์กร และแก้ไขเหตุละเมิดทางข้อมูลได้
7. จริยธรรมข้อมูล (Data Ethics) DPO ควรวิเคราะห์การวางกลยุทธ์ขององค์กร ขั้นตอนการดำเนินงาน และวิธีการประมวลผลข้อมูลให้เป็นไปตามหลักการอย่างเหมาะสม[5]

Singapore, "DPO Competency Framework and Training Roadmap," [Online] Accessed: 21 Oct 2563. Available from: https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap/Competencies#dpm

[5] สามารถอ่านแนวปฏิบัติเกี่ยวกับการปฏิบัติงานตามหลักจริยธรรมข้อมูล (Data Ethics) ได้ที่ OECD, "Good Practice Principles for Data Ethics in the Public Sector," [Online] Accessed: 31 Oct 2021.

8. การแลกเปลี่ยนข้อมูล (Data Sharing) หากองค์กรใดมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร DPO ควรสามารถที่จะประเมินคุณค่าของทรัพยากรข้อมูลเพื่อให้การดำเนินงานบรรลุเป้าหมายและวัตถุประสงค์ขององค์กร
9. การคิดเชิงออกแบบ (Design Thinking Practice) DPO ควรร่วมปลูกฝังและแนะแนวทางเพื่อให้ผู้มีส่วนเกี่ยวข้องภายในองค์กรมีการคิดเชิงออกแบบ เพื่อให้ผลิตภัณฑ์และการให้บริการตอบโจทย์ผู้บริโภคได้มากที่สุด หรือทำให้เกิดนวัตกรรมทางข้อมูลขึ้น

ถึงแม้ว่าจะมีการวางกรอบในการพัฒนาคุณสมบัติของ DPO ตามที่อธิบายข้างต้น เมื่อปัจจุบันยังไม่มีการประกาศกำหนดคุณสมบัติของ DPO อย่างเป็นทางการ ทำให้เกิดปัญหาว่าตำแหน่ง DPO เป็นผู้ที่มีความรู้ความเข้าใจ ทักษะ รวมถึงมีคุณสมบัติและการรับรองคุณวุฒิเป็นอย่างไร อาจเป็นไปได้ว่ากฎหมายเปิดโอกาสให้แต่ละภาคธุรกิจหรือแต่ละภาคอุตสาหกรรมกำหนดความสามารถของ DPO ตามความเหมาะสม ระดับความรู้ความเชี่ยวชาญ DPO อาจขึ้นอยู่กับปัจจัยต่างๆ ขององค์กรที่มีการแต่งตั้ง โดยอาจรวมถึงขนาดขององค์กร ปริมาณข้อมูลส่วนบุคคลที่ทำการจัดเก็บ ความอ่อนไหวของข้อมูล และความซับซ้อนในการประมวลผลข้อมูล

ในการเก็บรวบรวมข้อมูลเพื่อทำความเข้าใจปัญหาเชิงความสามารถของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน ผู้เขียนได้ทำการสัมภาษณ์ DPO ของสถาบันการเงินแต่ละแห่ง จำนวน 13 แห่ง ตามที่ได้กล่าวไว้แล้วในบทที่ 3 รวมถึงสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อทำให้ผู้เขียนเข้าใจบทบาทหน้าที่ของบุคคลภายในสถาบันการเงินที่เหมาะสมกับตำแหน่ง DPO และทราบว่า DPO ของสถาบันการเงินต้องมีความรู้ความเข้าใจด้านใดบ้าง และความรู้ความเข้าใจเหล่านั้นมีลักษณะอย่างไร มีความเฉพาะเจาะจงซึ่งแตกต่าง DPO ของภาคธุรกิจอื่นหรือไม่

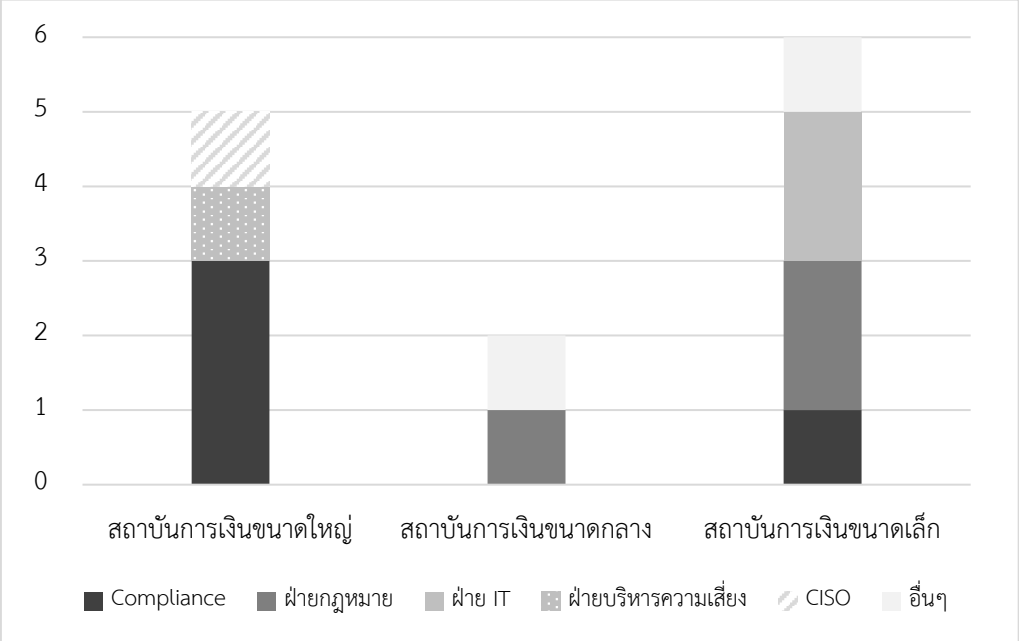
Available from: https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf. pp.7-9.

4.1 ฝ่ายงานหรือความรับผิดชอบของ DPO

ตามที่กล่าวมาแล้วในบทที่ 3 สถาบันการเงินมีคำสั่งแต่งตั้งให้บุคคลจากหน่วยงานหรือฝ่ายงานใดทำหน้าที่เป็น DPO ขององค์กรก็ได้ แต่บุคคลนั้นควรเป็นบุคลากรระดับผู้บริหาร ไม่ว่าจะเป็นผู้บริหารระดับต่ำ ระดับกลาง หรือระดับสูงของฝ่ายงานหรือส่วนงานก็ได้ เนื่องจากตำแหน่ง DPO จะต้องอยู่ในสถานะที่สามารถปฏิบัติหน้าที่และมีอำนาจตัดสินใจอย่างอิสระ (“หัวข้อ 3.3 ความเป็นอิสระ”) รวมถึงไม่ใช่บุคคลที่มีอำนาจตัดสินใจในการกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล อันนำมาซึ่งความขัดแย้งทางผลประโยชน์ (“หัวข้อ 3.4 ความขัดแย้งทางผลประโยชน์”) ทั้งนี้ การเรียกชื่อตำแหน่งบางตำแหน่งไม่อาจสรุปได้อย่างแน่นอนว่าบุคคลที่จะได้รับตำแหน่งนั้นจะสามารถเป็น DPO ไปด้วยในขณะเดียวกันได้หรือไม่ จึงต้องพิจารณาบทบาทหรือลักษณะงานของตำแหน่งดังกล่าวว่ามีความเป็นอิสระและมีความขัดแย้งทางผลประโยชน์หรือไม่

ในเบื้องต้นผู้เขียนทำการสัมภาษณ์ DPO ของสถาบันการเงินต่างๆ ว่าอยู่ในฝ่ายงาน/หน่วยงานใดหรือมีหน้าที่ความรับผิดชอบอื่นหรือไม่ ฝ่ายงานหรือความรับผิดชอบนั้นคืออะไร

ภาพที่ 8 ฝ่ายงานหรือความรับผิดชอบของ DPO ในสถาบันการเงิน



ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์ พบว่า[6] ในปัจจุบัน DPO ของสถาบันการเงินเป็นบุคลากรระดับผู้บริหารของฝ่ายงาน/ส่วนงานที่แตกต่างกันตามแต่ละองค์กร แบ่งออกเป็น ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) 4 ท่าน ฝ่ายกฎหมาย 3 ท่าน ฝ่ายเทคโนโลยีสารสนเทศ (IT) 2 ท่าน ฝ่ายบริหารความเสี่ยง 1 ท่าน ผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (CISO) 1 ท่าน และฝ่ายงานอื่นๆ อีก 2 ท่าน (ได้แก่ ฝ่ายกำกับดูแลข้อมูล และผู้ตรวจการธนาคาร)

4.2 ความรู้ความเข้าใจ

การแต่งตั้ง DPO ของสถาบันการเงินจะต้องคำนึงคุณสมบัติทางวิชาชีพของบุคคลใดบุคคลหนึ่ง โดยบุคคลที่ควรจะได้รับคัดเลือกเป็น DPO จะต้องมีความรู้ความเชี่ยวชาญในกฎหมายและแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงความสามารถที่จะดำเนินงานตามหน้าที่ที่กฎหมายกำหนดได้ลุล่วง[7] กล่าวคือ DPO ควรเป็นผู้ที่มีความรู้ความสามารถด้านต่างๆ ดังนี้

ตารางที่ 33 ความรู้ความเข้าใจที่จำเป็นต่อการปฏิบัติหน้าที่ DPO ของสถาบันการเงิน

ความรู้ความเข้าใจ ที่จำเป็นต่อการปฏิบัติหน้าที่ DPO	คำอธิบาย
1. กฎหมาย[8]	เนื่องจาก DPO มีหน้าที่ในการช่วยเหลือฝ่ายงานผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล รวมถึงบุคคลหรือหน่วยงานภายนอกที่จะนำข้อมูลส่วนบุคคลขององค์กรไปประมวลผลต่อ ซึ่งบางแห่งอาจมีการติดต่อสื่อสารกับหน่วยงานทั้งในและต่างประเทศ รวมถึงอาจมีการประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ DPO จึงต้องมีความรู้กฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลทั้งในประเทศ และต่างประเทศ เช่น GDPR หรือ PDPC ของประเทศสิงคโปร์ เพื่อให้สามารถนำวิธีปฏิบัติของต่างประเทศมาปรับใช้ให้เหมาะสมกับองค์กร นอกจากนี้ DPO ต้องมี

[6] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[7] GDPR, Article 43(3)

[8] Network of Data Protection Officers of the EU institution and bodies, Professional Standards for Data Protection Officers of the EU institution and bodies working under Regulation (EC) 45/2001. Ibid, pp.3-4.

ความรู้ความเข้าใจ ที่จำเป็นต่อการปฏิบัติหน้าที่ DPO	คำอธิบาย
	ความรู้กฎหมายและกฎเกณฑ์ในการทำงานของสถาบันการเงิน เช่น กฎหมายป้องกันและปราบปรามการฟอกเงิน กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับสถาบันการเงิน
2. ความเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กร[9]	โดยสภาพการทำงานของ DPO จะต้องมีการติดต่อประสานงาน และให้คำปรึกษากับฝ่ายงานผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล บุคคลหรือหน่วยงานภายนอกที่จะนำข้อมูลส่วนบุคคลขององค์กรไปประมวลผลต่อ รวมถึงหน่วยงานกำกับดูแลที่เกี่ยวข้อง ทำให้ DPO จำเป็นต้องเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลส่วนบุคคลองค์กรของสถาบันการเงินเป็นอย่างดี และอาจรวมถึงกระบวนการปฏิบัติงานของหน่วยงานที่สถาบันการเงินมีความสัมพันธ์ทางธุรกิจประกอบด้วย
3. การบริหารจัดการความเสี่ยง[10]	เนื่องด้วย DPO มีหน้าที่ต้องจัดทำการประเมินความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล และ DPIA ขององค์กร หรือให้คำปรึกษาในการร่างหลักเกณฑ์และการกรอกแบบฟอร์มเรื่องดังกล่าว รวมถึงมีหน้าที่เกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลตามที่กฎหมายกำหนด จึงมีความจำเป็นที่จะต้องมีประสบการณ์ในด้านการประเมินความเสี่ยงด้านความเป็นส่วนตัว เพื่อให้สามารถวิเคราะห์ได้ว่าลักษณะการใช้งานข้อมูลแต่ละอย่างขององค์กรมีความเสี่ยงที่อาจเกิดเหตุละเมิดของข้อมูลส่วนบุคคลมากน้อยเพียงใด หรืออาจผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างไรบ้าง และหาแนวทางการป้องกันหรือบรรเทาความเสี่ยงที่เหมาะสม
4. เทคโนโลยี[11]	ปัจจุบันสถาบันการเงินต่างนำเทคโนโลยีมาใช้กับระบบบริหารจัดการข้อมูลส่วนบุคคลขององค์กร DPO จะต้องเตรียมพร้อมในการรับภัยคุกคาม เข้าใจความเปลี่ยนแปลงและวิวัฒนาการของเทคโนโลยีที่จะทำให้ความเสี่ยงมีการพัฒนาเปลี่ยนแปลงรูปแบบไปจากเดิม รวมถึงสามารถประสานงาน

[9] ibid.

[10] Thomas Shaw, DPO Handbook Data Protection Officers Under the GDPR, Second ed. (The International Association of Privacy Professionals (IAPP), 2018). pp.12-16.

[11] ibid.

ความรู้ความเข้าใจ ที่จำเป็นต่อการปฏิบัติหน้าที่ DPO	คำอธิบาย
	และให้คำปรึกษากับฝ่ายงานต่างๆ โดยเฉพาะอย่างยิ่งกับฝ่ายงานเทคโนโลยีสารสนเทศในเบื้องต้น เช่น DPO ต้องเข้าใจระบบ IT ซึ่งรวมไปถึงสถาปัตยกรรม ระบบการรักษาความปลอดภัย การเชื่อมต่อไปยังอุปกรณ์ภายนอก หรือการใช้ Cloud service
5. มาตรฐานความปลอดภัยของข้อมูล[12]	จากสถิติพบว่าหนึ่งในเรื่องที่มีการกระทำความผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลบ่อยที่สุด คือ การที่องค์กรไม่มีมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสม[13] DPO จึงควรทำความเข้าใจมาตรฐานความปลอดภัยของข้อมูล (information security standard) ตัวอย่างเช่น ISO/IEC 27001 (ISMS), ISO/IEC 27701 (PIMS), NIST Privacy Framework เพื่อใช้เป็นแนวทางในการกำกับดูแลการจัดเก็บข้อมูลขององค์กรให้มีมาตรการคุ้มครองข้อมูลทางเทคนิค (Technical Measures) และเชิงองค์กร (Organizational Measures) เป็นไปตามกฎหมาย ไม่ว่าจะเป็นบุคคล กระบวนการทำงาน เครื่องมือ การจัดซื้อจัดจ้าง หรือกฎระเบียบภายในองค์กรที่เกี่ยวข้อง

ดังที่ผู้เขียนได้กล่าวไว้ใน “หัวข้อ 4.1 ฝ่ายงานหรือความรับผิดชอบของ DPO” ว่าปัจจุบัน DPO ของสถาบันการเงินต่างๆ มีความรับผิดชอบหรืออยู่ในฝ่ายงานที่แตกต่างกันไปตามแต่ละองค์กร โดยส่วนใหญ่จะอยู่ในฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ (compliance) ฝ่ายกฎหมาย และฝ่ายเทคโนโลยีสารสนเทศ (IT) เมื่อตำแหน่ง DPO เป็นตำแหน่งที่ต้องมีทักษะ ความรู้ความเข้าใจ

[12] Centre for Information Policy Leadership (CIPL), "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation," [Online] Accessed: 17 Oct 2020. Available from: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/11/final_cipl_gdpr_dpo_paper_17_november_2016.pdf. pp.23-24.

[13] CMS, "GDPR Enforcement Tracker," [Online] Accessed: 30 Oct 2021. Available from: https://www.enforcementtracker.com/?insights (เมื่อวันที่ 30 ตุลาคม 2564 จากข้อมูลสถิติเรื่องค่าปรับจากการฝ่าฝืน GDPR พบว่า องค์กรในประเทศที่อยู่ในสหภาพยุโรปถูกปรับจากการขาดมาตรการรักษาความปลอดภัยของข้อมูลบ่อยมากที่สุดเป็นอันดับสอง (176 ครั้ง รวมค่าปรับ 68,583,119 ยูโร) รองลงมาจากเรื่องการประมวลผลข้อมูลส่วนบุคคลโดยปราศจากฐานตามกฎหมาย)

หลากหลายด้านประกอบกัน ย่อมเป็นการยากลำบากที่จะหาบุคคลที่มีความรู้ความเข้าใจครอบคลุมทุกด้านได้ในบุคคลคนเดียว ทำให้มีความจำเป็นต้องจัดตั้งคณะทำงานขึ้นมาภายในองค์กรและส่งเสริมให้ DPO ศึกษาหาความรู้ในด้านที่จำเป็นต่อการปฏิบัติหน้าที่เพิ่มเติม

ผู้เขียนจึงทำการเก็บข้อมูลจากการตอบแบบสอบถามของ DPO และบุคคลที่เกี่ยวข้องของสถาบันการเงินจำนวน 13 แห่งต่อไปว่า DPO ของแต่ละองค์กรมีความต้องการเพิ่มพูนความรู้ความเข้าใจในด้านใดบ้าง หากมีความต้องการมากกว่า 1 ด้าน ให้ผู้ตอบแบบสอบถามเรียงลำดับความต้องการเพิ่มพูนความรู้ความเข้าใจเหล่านั้น หลังจากนั้นผู้เขียนได้ทำสัมภาษณ์เพิ่มเติมว่าเพราะเหตุใดความรู้ความเข้าใจด้านนั้นจึงสำคัญต่อการปฏิบัติหน้าที่ในฐานะ DPO

ผลการศึกษาพบว่า[14] DPO ของสถาบันการเงินแต่ละแห่งในประเทศไทยกล่าวถึง และให้ความสำคัญกับความต้องการเพิ่มพูนความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละด้าน ดังตารางด้านล่างต่อไปนี้

ตารางที่ 34 ความต้องการเพิ่มพูนความรู้ความใจของ DPO ในสถาบันการเงินที่ผู้ให้สัมภาษณ์กล่าวถึง

ความรู้ความเข้าใจด้านที่ต้องการ	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
กฎหมาย	4	2	4
มาตรฐานความปลอดภัยของข้อมูล	3	2	6
เทคโนโลยี	3	2	5
การบริหารจัดการความเสี่ยง	3	2	3
การดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กร	3	2	3

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

โดย DPO ทำการประเมินอันดับความสำคัญของความต้องการเพิ่มพูนความรู้ความเข้าใจในแต่ละด้านที่จำเป็นต่อการปฏิบัติหน้าที่ DPO ให้เป็นไปตามกฎหมาย ดังปรากฏตามอันดับดังต่อไปนี้

[14] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ตารางที่ 35 อันดับความรู้ความเข้าใจที่ต้องการเพิ่มพูนของ DPO ในสถาบันการเงินที่ผู้ให้สัมภาษณ์ทำการประเมิน

อันดับของความต้องการ	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
1	กฎหมาย (3) เทคโนโลยี (1)	กฎหมาย (2)	กฎหมาย (3) มาตรฐานฯ (2) เทคโนโลยี (2) บริหารความเสี่ยง (1)
2	มาตรฐานฯ (1) เทคโนโลยี (1) ความเข้าใจองค์กร (1)	เทคโนโลยี (1) ความเข้าใจองค์กร (1)	มาตรฐานฯ (3) เทคโนโลยี (1) บริหารความเสี่ยง (1)
3	กฎหมาย (1) มาตรฐานฯ (2) บริหารความเสี่ยง (1)	มาตรฐานฯ (1) บริหารความเสี่ยง (1)	มาตรฐานฯ (1) บริหารความเสี่ยง (1) ความเข้าใจองค์กร (1)
4	เทคโนโลยี (1) บริหารความเสี่ยง (1) ความเข้าใจองค์กร (1)	มาตรฐานฯ (1) ความเข้าใจองค์กร (1)	เทคโนโลยี (2) ความเข้าใจองค์กร (1)
5	บริหารความเสี่ยง (1) ความเข้าใจองค์กร (1)	เทคโนโลยี (1) บริหารความเสี่ยง (1)	กฎหมาย (1) ความเข้าใจองค์กร (1)

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

4.2.1 กฎหมาย

จากแบบสอบถามพบว่า[15] กฎหมายเป็นความรู้ความเข้าใจในด้านที่ถูกกล่าวถึงโดย DPO ของสถาบันการเงินจำนวน 10 แห่ง (ขนาดใหญ่ 4 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 4 แห่ง) ซึ่ง DPO ของสถาบันการเงินขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่งและขนาดเล็ก 3 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่สาม และ

[15] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้ความรู้ความเข้าใจด้านกฎหมายเป็นสิ่งที่ DPO ของสถาบันการเงินต้องการเพิ่มพูนมากที่สุดเป็น *'อันดับแรก'*

จากการสัมภาษณ์ ผู้ให้สัมภาษณ์ของสถาบันการเงินที่เห็นว่าความรู้กฎหมายมีความสำคัญต่อ DPO ได้ให้เหตุผลที่สำคัญไว้ ดังต่อไปนี้[16]

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า "เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องใหม่และมีลักษณะเป็นกฎหมายเทคนิคสูง ประกอบกับมีความแตกต่างจาก GDPR ซึ่งเป็นกฎหมายต้นแบบของสหภาพยุโรป และปัจจุบันยังไม่มีกฎหมายลำดับรอง จึงทำให้ยากต่อการทำความเข้าใจและการนำมาปฏิบัติ DPO จึงจำเป็นต้องทำความเข้าใจทั้งเนื้อหาและเจตนารมณ์เพื่อให้สถาบันการเงินดำเนินการให้เป็นไปตามกฎหมายได้อย่างถูกต้องครบถ้วน"
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า "หากสถาบันการเงินไม่เข้าใจวัตถุประสงค์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างลึกซึ้ง ก็ไม่สามารถกำหนดหลักการบริหารจัดการข้อมูลส่วนบุคคลได้อย่างครบถ้วนสมบูรณ์"
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า "เนื่องจากกิจกรรมบางอย่างอาจเกี่ยวข้องกับเจ้าของข้อมูลซึ่งเป็นชาวต่างชาติ DPO จำเป็นต้องเพิ่มพูนทักษะความรู้เรื่อง แนวปฏิบัติสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่ได้รับการยอมรับ (white-list) อย่างอังกฤษ อเมริกา ญี่ปุ่น ฮ่องกง หรือสิงคโปร์ เพื่อกำหนดนโยบายและแนวทางการจัดการอย่างสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลกับการนำข้อมูลไปใช้ให้เกิดประโยชน์สูงสุด เช่น ในประเทศอังกฤษมีการนำข้อมูลการชำระหนี้ค่าสินค้าออนไลน์มาพิจารณาความน่าเชื่อถือทางการเงินของลูกหนี้เงินกู้"

[16] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

4.2.2 มาตรฐานความปลอดภัยของข้อมูล

จากแบบสอบถามพบว่า[17] มาตรฐานความปลอดภัยของข้อมูลเป็นความรู้ความเข้าใจในด้านที่ถูกกล่าวถึงโดย DPO ของสถาบันการเงินจำนวน 11 แห่ง (ขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 6 แห่ง) ซึ่ง DPO ของสถาบันการเงินขนาดขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 3 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 2 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้ความรู้ความเข้าใจด้านมาตรฐานความปลอดภัยของข้อมูล เป็นความรู้ความเข้าใจที่ DPO ของสถาบันการเงินต้องการเพิ่มพูนเป็น *‘อันดับสอง’*

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงินที่เห็นว่าความรู้ด้านมาตรฐานความปลอดภัยของข้อมูลมีความสำคัญต่อ DPO ให้เหตุผลที่สำคัญ ดังต่อไปนี้[18]

- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งเห็นว่า “เนื่องจากประเด็นการฟ้องร้องคดีข้อมูลส่วนบุคคลมักเป็นเรื่องเหตุละเมิดข้อมูลส่วนบุคคล (data breach) หรือการรั่วไหลของข้อมูล (data leakage) ตำแหน่ง DPO ต้องเข้าใจมาตรฐานความปลอดภัยของข้อมูล เพื่อกำกับดูแลระบบบริหารจัดการข้อมูลของสถาบันการเงินให้เป็นไปตามตามมาตรฐานที่กฎหมายหรือมาตรฐานสากลรับรอง”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “DPO ต้องมีความรู้เรื่องมาตรฐานฯ และเข้าใจว่ามาตรฐานฯ นั้นมีความสัมพันธ์กับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างไร เพื่อให้สามารถทำความเข้าใจระบบบริหารจัดการข้อมูลองค์กร ตรวจสอบ ให้คำแนะนำ และทำงานร่วมกับหน่วยงานที่รับผิดชอบตามมาตรฐาน ISO ได้”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “DPO ควรมีความรู้พื้นฐานในเรื่องมาตรฐานฯ สามารถเชื่อมโยงกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับ Cybersecurity ได้ ระบุได้ว่าองค์กรมีระบบย่อยใดมารองรับ เช่น ระบบบริหาร

[17] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[18] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

จัดการการขอความยินยอม (Consent Management) ระบบป้องกันการรั่วไหลของข้อมูล (Data Leak Protection) ระบบจัดการการแจ้งเตือนและขอความยินยอมในการเก็บคุกกี้ (Cookie Management) ฯลฯ เพื่อศึกษาแนวทางและการเตรียมความพร้อมในการรับมือกับภัยคุกคามต่อสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลที่อาจเกิดขึ้น”

4.2.3 เทคโนโลยี

จากแบบสอบถามพบว่า[19] เทคโนโลยีเป็นความรู้ความเข้าใจในด้านที่ถูกกล่าวถึงโดย DPO ของสถาบันการเงินจำนวน 10 แห่ง (ขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 5 แห่ง) ซึ่ง DPO ของสถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดใหญ่ 1 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 1 แห่งขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้ความรู้ความเข้าใจด้านเทคโนโลยี เป็นความรู้ความเข้าใจที่ DPO ของสถาบันการเงินต้องการเพิ่มพูนเป็น *‘อันดับสาม’*

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงินที่เห็นว่าความรู้ด้านเทคโนโลยีมีความสำคัญต่อ DPO ให้เหตุผลที่สำคัญ ดังต่อไปนี้[20]

- DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งกล่าวว่า “DPO ต้องทราบว่าข้อมูลส่วนบุคคลของลูกค้าถูกจัดเก็บไว้ในรูปแบบใดบ้าง ปัจจุบันสถาบันการเงินต่างนำเทคโนโลยีมาใช้กับระบบบริหารจัดการข้อมูลส่วนบุคคลขององค์กร เช่น ระบบบริหารจัดการความยินยอม การบริหารจัดการสิทธิของเจ้าของข้อมูล (ลูกค้าขอเปลี่ยนแปลงหรือขอลบข้อมูลของตน)”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “เนื่องจากกฎหมายไม่ได้กำหนดรายละเอียดเรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลที่

[19] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[20] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

เหมาะสมไว้อย่างชัดเจน DPO จึงต้องมีความรู้และเข้าใจความเปลี่ยนแปลงและวิวัฒนาการของเทคโนโลยีที่จะอาจก่อให้เกิดผลกระทบต่อข้อมูลส่วนบุคคล เพื่อพิจารณาว่าระบบรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่สถาบันการเงินมีอยู่นั้นมีความปลอดภัยและได้มาตรฐานมากน้อยเพียงใด”

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “ในทางปฏิบัติ DPO ต้องประสานงานและให้คำปรึกษาเบื้องต้นกับหน่วยงานธุรกิจและฝ่าย IT เกี่ยวกับการใช้เทคโนโลยีอย่างสม่ำเสมอ เช่น การให้คะแนนเครดิตทางเลือก (alternative credit scoring) หรือการวิเคราะห์ข้อมูลเพื่อหาแนวโน้มพฤติกรรมของกลุ่มเป้าหมาย (data analytic)”

4.2.4 การบริหารจัดการความเสี่ยง

จากแบบสอบถามพบว่า[21] การบริหารจัดการความเสี่ยงเป็นความรู้ความเข้าใจในด้านที่ถูกกล่าวถึงโดย DPO ของสถาบันการเงินจำนวน 8 แห่ง (ขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่ง DPO ของสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่หนึ่ง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดใหญ่ 1 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินขนาดใหญ่ 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินใหญ่ 1 แห่ง และขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้ความรู้ความเข้าใจด้านการบริหารจัดการความเสี่ยงเป็นความรู้ความเข้าใจที่ DPO ของสถาบันการเงินต้องการเพิ่มพูนเป็น *‘อันดับสี่’*

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงินที่เห็นว่าความรู้ด้านการบริหารจัดการความเสี่ยงมีความสำคัญต่อ DPO ให้เหตุผลที่สำคัญ ดังต่อไปนี้[22]

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “เนื่องจากเรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นประเด็นใหม่ของธุรกิจสถาบันการเงิน และก่อให้เกิดความเสี่ยง

[21] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[22] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

หลายด้าน ทำให้ในบางครั้ง DPO อาจมองไม่เห็นถึงความเสี่ยงบนพื้นฐานข้อเท็จจริงที่เกิดขึ้น และไม่สามารถจัดการกับความเสี่ยงเหล่านั้นได้อย่างเพียงพอเพื่อให้เป็นไปตามกฎหมาย”

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “เมื่อธนาคารพาณิชย์นำข้อมูลส่วนบุคคลของลูกค้ามาใช้ในการออกผลิตภัณฑ์หรือการให้บริการใหม่ DPO ต้องสามารถวิเคราะห์ได้ว่ากิจกรรมการใช้ข้อมูลส่วนบุคคลเหล่านั้นมีความเสี่ยงอย่างไรบ้าง เพื่อให้คำปรึกษาในการร่างหลักเกณฑ์และการจัดทำแบบฟอร์ม DPIA กับฝ่ายความเสี่ยง เช่น หากเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงสถาบันการเงินจะมีหน้าที่ต้องแจ้งต่อสำนักงาน เจ้าของข้อมูล หรือหน่วยงานกำกับดูแล”

อนึ่ง ผู้ให้สัมภาษณ์ของสถาบันการเงินหลายท่านได้กล่าวถึงความไม่ชัดเจนของเกณฑ์ที่ใช้กำหนดระดับความเสี่ยงของข้อมูลส่วนบุคคล และต้องการตัวอย่างในทางปฏิบัติ

4.2.5 การดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กร

จากแบบสอบถามพบว่า[23] ความเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กรเป็นความรู้ความเข้าใจในด้านที่ถูกกล่าวถึงโดย DPO ของสถาบันการเงินจำนวน 8 แห่ง (ขนาดใหญ่ 3 แห่ง ขนาดกลาง 2 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่ง DPO ของสถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับที่สอง สถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สาม สถาบันการเงินใหญ่ 1 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่สี่ สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับที่ห้า ด้วยเหตุนี้ ผู้เขียนจึงจัดอันดับให้ความเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กร เป็นสิ่งที่ DPO ของสถาบันการเงินต้องการเพิ่มพูนเป็น *‘อันดับห้า’*

จากการสัมภาษณ์พบว่า ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งที่เห็นว่าความเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลขององค์กรมีความสำคัญต่อ DPO ให้เหตุผลว่า “DPO จำเป็นต้องเข้าใจการดำเนินธุรกิจของสถาบันการเงิน โดยเฉพาะอย่างยิ่งความเข้าใจ

[23] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

เกี่ยวกับรูปแบบธุรกิจ ผลิตภัณฑ์ และการให้บริการต่างๆ ของแต่ละสถาบันการเงินที่ปัจจุบันเพิ่มขึ้นอย่างต่อเนื่องตลอดเวลา เพื่อให้สามารถให้คำปรึกษาและยกตัวอย่างที่เข้าใจได้ง่ายต่อความเข้าใจแก่แต่ละฝ่ายงาน รวมถึงตรวจสอบไม่ให้กิจกรรมการประมวลผลข้อมูลรุกล้ำสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูล”[24]

4.2.6 มาตรการรักษาความปลอดภัยข้อมูลเชิงองค์กร กับ มาตรการรักษาความปลอดภัยข้อมูลเชิงเทคนิค

ความรู้ด้านมาตรฐานความปลอดภัยข้อมูล (Information Security Standard) ของ DPO ตาม “หัวข้อ 4.2.2 มาตรฐานความปลอดภัยของข้อมูล” มีความสำคัญต่อหน้าที่ในการให้คำแนะนำ และตรวจสอบมาตรการรักษาความปลอดภัยของข้อมูลของสถาบันการเงินเป็นไปตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด ซึ่งอาจรวมถึง[25]

- การแฝงข้อมูล (pseudonymization)
- การเข้ารหัสข้อมูลส่วนบุคคล (encryption)
- การทำให้แน่ใจว่าสามารถรักษาความมั่นคงปลอดภัยของระบบหรือบริการประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบไปด้วยการธำรงไว้ซึ่งความลับ (confidentiality)[26] ความถูกต้องครบถ้วน (integrity)[27] และสภาพพร้อมใช้

[24] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[25] GDPR, Article 32(1) และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1) และร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล ข้อ 2.3. โปรดดู https://www.law.chula.ac.th/event/10941/

[26] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guildlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 530-531. (ตัวอย่างเหตุการณ์ที่ทำให้เกิดการสูญเสียความลับของข้อมูลส่วนบุคคล (confidentiality) เช่น เอกสารหรือแฟลชไดร์ฟที่มีข้อมูลส่วนบุคคลสูญหายระหว่างขนส่ง หรือถูกนำไปใช้งานต่อโดยไม่ได้ทำลายข้อมูลก่อน ข้อมูลส่วนบุคคลถูกส่งไปยังที่อยู่ที่ไม่ถูกต้อง การตั้งค่าเว็บไซต์หรือบริการคลาวด์ผิดทำให้ข้อมูลส่วนบุคคลถูกเข้าถึงจากสาธารณะได้)

[27] ibid. (ตัวอย่างเหตุการณ์ที่มีผลกระทบทำให้ข้อมูลขาดความถูกต้องครบถ้วน (integrity) เช่น ข้อมูลที่ถูกเก็บไว้ในระบบฐานข้อมูลถูกแก้ไขจากผู้ไม่มีสิทธิ หรือข้อมูลในระบบทะเบียนประวัติลูกค้าเสียหายจากการ

งาน (availability)[28] หรือที่เป็นที่รู้จักกันในชื่อ Confidentiality, Integrity and Availability (CIA Triad)

- ความสามารถในการกู้คืนระบบ หรือบริการที่มีการประมวลผลข้อมูลส่วนบุคคลให้กลับมาพร้อมให้บริการได้ทันการณ์หากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น
- กระบวนการทดสอบและประเมินความมีประสิทธิภาพและประสิทธิผลของมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures)

จะเห็นได้ว่า DPO ในสถาบันการเงินต้องมีความรู้ความเข้าใจด้านมาตรฐานความปลอดภัยของข้อมูล ซึ่งแบ่งแยกออกเป็นความรู้ความเข้าใจ 2 ด้าน ได้แก่ (1) มาตรการเชิงองค์กร (Organizational Measures) และ (2) มาตรการเทคนิค (Technical Measures) โดยการติดตามตรวจสอบความเหมาะสมของมาตรการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล DPO ต้องคำนึงถึง สภาพและลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ความเสี่ยงของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ขนาดและความซับซ้อนของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ภาระและต้นทุนในการดำเนินการ[29]

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่ บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ และแจ้งเตือนเมื่อมีการแก้ไขปรับปรุงมาตรการดังกล่าว รวมถึง สร้างเสริมความ

ประมวลผลที่ผิดพลาดของโปรแกรมคอมพิวเตอร์ ทำให้ประเมินสินเชื่อเงินกู้ผิดพลาด จำเป็นต้องใช้ข้อมูลจากเอกสารทดแทน ทำให้การปฏิบัติงานล่าช้า)

[28] ibid. (ความพร้อมใช้ (Availability) คือการทำให้ผู้ที่มีสิทธิสามารถเข้าถึงและใช้ข้อมูลได้เมื่อมีความต้องการในการใช้งาน สามารถป้องกันข้อมูลเสียหายหรือสูญหาย ซึ่งอาจเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลหรืออาจก่อให้เกิดความรำคาญแก่เจ้าของข้อมูล เช่น ไฟล์ Excel ที่เก็บข้อมูลลูกค้าเกิดความเสียหาย เนื่องจากโปรแกรม Windows หรือโปรแกรม Microsoft Word ทำงานผิดพลาด)

[29] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล ข้อ 2.5. โปรดดู https://www.law.chula.ac.th/event/10941/

ตระหนักรู้ ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด[30]

ผู้เขียนได้สัมภาษณ์ DPO ของสถาบันการเงินทั้ง 13 แห่งถึงความสำคัญของมาตรการรักษาความปลอดภัยข้อมูลเชิงองค์กร และมาตรการเชิงเทคนิค โดยมีคำถามว่า “ระหว่างมาตรการทั้งสอง ท่านมีความเห็นว่ามาตรการใดมีความสำคัญต่อตำแหน่ง DPO ในแง่ของความรู้ความเข้าใจมากกว่ากัน เพราะเหตุใด”

ตารางที่ 36 ความรู้มาตรการรักษาความปลอดภัยข้อมูลด้านที่สำคัญต่อการปฏิบัติงานในตำแหน่ง DPO ในสถาบันการเงิน (ระหว่างมาตรการเชิงองค์กร กับ มาตรการเชิงเทคนิค)

ความเห็นของผู้ให้สัมภาษณ์	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
มาตรการเชิงองค์กรสำคัญมากกว่า	3	1	3
มาตรการเชิงเทคนิคสำคัญมากกว่า	-	1	-
ทั้งสองด้านมีความสำคัญเท่าๆ กัน	2	-	1
หมายเหตุ: เนื่องจากมีเวลาจำกัดในการสัมภาษณ์ ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดเล็กจำนวน 2 แห่งจึงไม่ได้แสดงความเห็นในเรื่องดังกล่าว			

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ผลการสัมภาษณ์พบว่า[31] DPO ของสถาบันการเงินจำนวน 7 แห่ง มีความเห็นว่ามาตรการรักษาความปลอดภัยข้อมูลเชิงองค์กร มีความสำคัญในแง่ของความรู้ความเข้าใจของ DPO มากกว่า ในขณะที่ DPO ของสถาบันการเงินขนาดกลาง 1 แห่ง เห็นว่าความรู้ด้านมาตรการเชิงเทคนิค มีความสำคัญมากกว่า และ DPO ของสถาบันการเงิน 3 แห่งเห็นว่ามาตรการทั้งสองด้านมีความสำคัญต่อ DPO ในแง่ของความรู้ความเข้าใจเท่าๆ กัน (ทั้งนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดเล็กอีก 2 แห่งจึงไม่ได้แสดงความเห็นในเรื่องนี้ไว้ เนื่องจากมีเวลาจำกัด)

ผู้ให้สัมภาษณ์ที่มีความเห็นว่าความเข้าใจมาตรการเชิงบริหารจัดการองค์กร (Organizational Measures) มีความสำคัญมากกว่า (7 แห่ง) ให้เหตุผลที่สำคัญไว้ดังต่อไปนี้[32]

---

[30] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล ข้อ 2.3. โปรดดู https://www.law.chula.ac.th/event/10941/

[31] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[32] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “ปัจจุบันสถาบันการเงินต่างๆ มีการออกแบบผลิตภัณฑ์ และการบริการที่ตอบโจทย์ลูกค้าเป็นจำนวนมาก การที่ DPO มีความรู้ด้านมาตรการเชิงองค์กรจะทำให้สามารถเข้ามามีส่วนร่วมในการบริหารจัดการและให้ข้อเสนอแนะเกี่ยวกับกิจกรรมการประมวลผล เพื่อให้องค์กรสามารถปฏิบัติตามกฎหมาย พร้อมทั้งสามารถแข่งขันทางธุรกิจในยุคดิจิทัลได้”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งเห็นว่า “เมื่อทำความเข้าใจมาตรการเชิงบริหารจัดการองค์กรได้ DPO จะสามารถให้คำแนะนำตั้งแต่การออกแบบโครงสร้างองค์กรให้เหมาะสม กำหนดบทบาทหน้าที่ความรับผิดชอบ ประเมินและจัดการความเสี่ยงให้เหมาะสมกับการดำเนินธุรกิจขององค์กร รวมถึงให้คำปรึกษาเกี่ยวกับความต้องการเครื่องมือหรือเทคโนโลยีได้ ฉะนั้นมาตรการเชิงเทคนิคก็มีความสำคัญและจำเป็นลดลง”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “DPO ต้องให้ความสำคัญกับการทำความเข้าใจภาพรวมการรักษาความปลอดภัยข้อมูลขององค์กรเสียก่อน ส่วนมาตรการเชิงเทคนิคมีความสำคัญรองลงมาและไม่จำเป็นต้องมีความเข้าใจอย่างลึกซึ้ง เนื่องจากสามารถสอบถามและมอบหมายให้ฝ่าย IT ดำเนินการได้อยู่แล้ว”
- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งเห็นว่า “ความรู้เข้าใจมาตรการเชิงบริหารจัดการองค์กรของ DPO มีความสำคัญต่อการตรวจสอบระบบรักษาความปลอดภัยข้อมูลขององค์กรให้เป็นไปตามหลักการ 7 Layers of Cybersecurity”

ในขณะที่ผู้ให้สัมภาษณ์ที่มีความเห็นว่าความเข้าใจมาตรการเชิงเทคนิค (Technical Measures) มีความสำคัญมากกว่า (1 แห่ง) ให้เหตุผลดังนี้[33]

- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่ง กล่าวว่า “เนื่องจากมาตรการเชิงเทคนิคที่เกี่ยวกับการรักษาความปลอดภัยข้อมูลมีความซับซ้อนมากกว่า และปัจจุบันข้อมูลอยู่ในรูปอิเล็กทรอนิกส์มากกว่าอยู่ในรูปของเอกสาร DPO จึงจำเป็นต้องเข้าใจมาตรการเชิงเทคนิคเพื่อจะได้กำกับดูแลให้องค์กรสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างถูกต้อง”

[33] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ส่วนผู้ให้สัมภาษณ์ที่มีความเห็นว่าทั้งความเข้าใจด้านมาตรการเชิงบริหารจัดการองค์กร และมาตรการเชิงเทคนิค มีความสำคัญเท่าๆ กัน (3 แห่ง) ให้เหตุผลที่สำคัญดังต่อไปนี้[34]

- เจ้าหน้าที่ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “DPO ต้องเริ่มทำความเข้าใจมาตรการเชิงองค์กรที่อยู่ภายใต้การกำกับดูแลของ ธปท. และ กลต. ต่อมาจึงทำความเข้าใจมาตรการเชิงเทคนิค โดยระดับความเข้าใจขึ้นอยู่กับรูปแบบและความซับซ้อนของการดำเนินธุรกิจของธนาคาร เช่น หากธนาคารให้บริการดิจิทัลหลากหลายรูปแบบ DPO ควรจะมีความเข้าใจทางเทคนิคที่ลึกซึ้งมากกว่าปกติ”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเห็นว่า “ทั้งสองมาตรการมีความสำคัญเท่ากัน อันดับแรก DPO ต้องทราบว่าองค์กรใช้เครื่องมือใดในการรักษาความปลอดภัยข้อมูลบ้าง เครื่องมือเหล่านั้นทำงานอย่างไร และมีความเสี่ยงหรือจุดอ่อนอย่างไรบ้าง ซึ่งฝ่าย IT จะเป็นผู้พิจารณาเลือกเครื่องมือและขอคำปรึกษาหารือกับ DPO โดย DPO ต้องสามารถออกแบบ กำกับดูแล และตรวจสอบการรักษาความปลอดภัยข้อมูลขององค์กรได้”
- DPO ของสถาบันการเงินขนาดกลางแห่งหนึ่งเห็นว่า “มาตรการเชิงองค์กรและมาตรการเชิงเทคนิคต่างมีความสำคัญต่อ DPO เพราะต้องให้ความสำคัญกับการกำหนดโครงสร้างองค์กรและกระบวนการบริหารจัดการความเสี่ยงที่เหมาะสม โดยมาตรการเชิงเทคนิคมีความสำคัญเนื่องจากความปลอดภัยของข้อมูลกับความเป็นส่วนตัวนั้น มีหลักการหลายเรื่องที่สอดคล้องกัน เช่น CIA Triad – Confidentiality, Integrity, Availability สถาบันการเงินมีหน้าที่ในการพัฒนาเครื่องมือขึ้นมาเพื่อจัดการเรื่องดังกล่าว เช่น DLP Software, Firewall, Identity Access Management”

4.3 การรับรองคุณวุฒิ (Certification)

ปัจจุบันองค์กรด้านสิทธิในความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานกำกับดูแลที่เกี่ยวข้องทั่วโลก มีการพัฒนาหลักสูตรฝึกอบรมและการจัดสัมมนาแก่บุคคลที่ต้องการ

[34] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ประกอบอาชีพ DPO เป็นจำนวนมาก และเมื่อบุคคลใดสอบผ่านการฝึกอบรมก็จะได้ใบรับรองคุณวุฒิ (Certificate) ซึ่งหลักสูตรการฝึกอบรมของสมาคมวิชาชีพด้านสิทธิในความเป็นส่วนตัวระหว่างประเทศ (International Association of Privacy Professional - IAPP) เป็นหลักสูตรที่ปัจจุบันได้รับการยอมรับอย่างกว้างขวาง เช่น Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Manager (CIPM)[35] อย่างไรก็ดี ถึงแม้หลักสูตรและการฝึกบอบรมดังกล่าวจะมีวัตถุประสงค์ในการพัฒนาบุคคลที่จะทำหน้าที่เป็น DPO ให้มีความรู้ความเชี่ยวชาญในระดับที่เป็นไปตามที่ GDPR หรือแนวปฏิบัติที่เกี่ยวข้องกำหนด แต่ไม่มีกฎหมายใดกำหนดรายละเอียดที่ชัดเจนว่าต้องฝึกอบรมหรือมีใบรับรองคุณวุฒิด้านใดบ้าง บรรดาหลักสูตรฝึกอบรมและการรับรองคุณวุฒิของหน่วยงานต่างๆ จึงเป็นเพียงปัจจัยอย่างหนึ่งที่แต่ละองค์กรใช้ในการคัดเลือกความสามารถของบุคคลที่จะเข้ามาดำรงตำแหน่ง DPO หาใช่สิ่งที่กฎหมายกำหนดไว้เป็นเงื่อนไขไม่[36] ด้วยเหตุนี้ แต่ละประเทศจึงสามารถกำหนดกรอบการพัฒนาหลักสูตรการฝึกอบรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นได้อย่างอิสระ[37]

สำหรับประเทศไทยได้มีการกำหนดกรอบแนวทางการพัฒนากฎหมายเกี่ยวกับความสามารถและการฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Competency Framework and Training Roadmap) ดังที่กล่าวไปในตอนต้นของบทที่ 4 อนึ่ง ในส่วนของการรับรองคุณสมบัติของ DPO ในประเทศไทยนั้นผู้เขียนจะกล่าวถึงต่อไปใน “หัวข้อ 4.6.1 การรับรองคุณสมบัติของ DPO”

เพื่อค้นหาแนวทางในการพัฒนาหลักสูตรฝึกอบรมสำหรับ DPO และผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินในประเทศไทย ผู้เขียนได้สอบถามผู้ให้สัมภาษณ์ของสถาบันการเงินจำนวน 13 แห่งว่าปัจจุบัน DPO ของสถาบันการเงินได้รับใบรับรองคุณวุฒิ (Certificate) เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ อะไรบ้าง และคิดว่าควรจะสอบได้อะไร

---

[35] IAPP, "Get DPO Ready: Training and Resources," [Online] Accessed: 20 Jan 2021. Available from: https://iapp.org/train/Data-protection-training/

[36] Garante per la Protezione dei Dati Personali, "FAQs on DPO," [Online] Accessed: 20 Jan 2021. Available from: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793 (Available in Italian only)

[37] ผู้เขียนเรียบเรียงจาก Douwe Korff, and Marie Georges. Ibid, pp.128-129.

เพิ่มเติม รวมถึงความเห็นที่มีต่อการสอบรับรองคุณวุฒิเกี่ยวกับการปฏิบัติหน้าที่ DPO ซึ่งจัดขึ้นโดยหน่วยงานและองค์กรต่างๆ ในประเทศไทยในปัจจุบัน

ตารางที่ 37 จำนวน DPO ผู้ให้สัมภาษณ์ที่มีใบรับรองคุณวุฒิ (Certificate)

ใบรับรองคุณวุฒิ	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
มีใบรับรองคุณวุฒิ	2	2	2
ไม่มีใบรับรองคุณวุฒิ	3	-	4

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์[38] พบว่า DPO ที่มีใบรับรองคุณวุฒิที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลมีจำนวน 6 ท่าน ส่วนใหญ่ใบรับรองคุณวุฒิที่บุคคลดังกล่าวได้รับมักจะเป็นใบรับรองคุณวุฒิที่ถูกออกโดยองค์กรต่างประเทศ มีบางรายเท่านั้นที่มีใบรับรองคุณวุฒิจากหน่วยงานภายในประเทศไทย ส่วน DPO ของสถาบันการเงิน 7 ท่าน ยังไม่มีใบรับรองคุณวุฒิดังกล่าว

โดยใบรับรองคุณวุฒิที่ DPO ของสถาบันการเงินข้างต้น (6 ท่าน) ได้รับมีดังต่อไปนี้

ตารางที่ 38 ใบรับรองคุณวุฒิเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ DPO ของสถาบันการเงินได้รับ

- CEPAS: Data Protection Officer by ACIS Professional Center (4 ท่าน)
- Certified Information Privacy Professional (CIPP) (2 ท่าน)
- Certify Information Systems Security Professional (CISSP) (1 ท่าน)
- Certified Information Security Manager (CISM) ISACA Greater Washington (1 ท่าน)
- Certified Chief Information Officer (CIO) National Defense University (1 ท่าน)
- Certified Chief Information Security Officer (CCISO) National Defense University (1 ท่าน)
- GDPR Data Protection Officer Skills by University of Derby (1 ท่าน)
- Certificate จากการอบรม Privacy and Security Summit (1 ท่าน)
- Certificate จากการอบรม Personal Data Protection Act-PDPA#1 (1 ท่าน)
- หลักสูตรกฎหมายคุ้มครองข้อมูลส่วนบุคคล ของมหาวิทยาลัยในประเทศไทย (2 ท่าน)

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

[38] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ทั้งนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินต่างๆ มีความเห็นที่สำคัญเกี่ยวกับการจัดฝึกอบรมหลักสูตรของหน่วยงานหรือองค์กรต่างๆ ในประเทศไทย ดังนี้[39]

- เจ้าหน้าที่อาวุโสฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “การอบรมเกี่ยวกับการปฏิบัติงานของ DPO ในประเทศไทยขาดการรับรองที่ชัดเจน หรือยังไม่อยู่ในระดับที่ได้มาตรฐานเมื่อเปรียบเทียบกับหลักสูตรของต่างประเทศ โดยหลักสูตรการฝึกอบรมและใบรับรองคุณวุฒิอาจมีความแตกต่างกันในแต่ละสถาบันการเงิน ซึ่งต้องตรงกับหน้าที่ความรับผิดชอบที่ DPO มีต่อองค์กรที่ตนได้รับการแต่งตั้ง เช่น วิธีการค้นหาข้อมูลส่วนบุคคลภายในองค์กร หรือการทำ ROPA”
- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งซึ่งอยู่ในส่วนงานบริหารความเสี่ยงองค์กรกล่าวว่า “ยังไม่มีใบรับรองดังกล่าวและเห็นว่ายังไม่มีความจำเป็น เนื่องจากตนมีหน้าที่ดูแลความเสี่ยงทั้งหมดไม่เฉพาะแต่ความเสี่ยงที่เกิดขึ้นจากข้อมูลส่วนบุคคล และปัจจุบันกฎหมายยังไม่มีการกำหนดคุณสมบัติของ DPO ไว้ แต่ได้ส่งเสริมให้คณะทำงานฯ เข้ารับการฝึกอบรมในหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลที่เป็นที่ยอมรับในระดับสากล เช่น หลักสูตรของสถาบันมาตรฐานอังกฤษ (BSI) และ CIPP/E (Certified Information Privacy Professional) ของสหภาพยุโรป รวมถึง ISO ต่างๆ”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “กำลังรอสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สนค.) ออกประกาศกำหนดคุณสมบัติของ DPO และกำหนดหลักสูตรที่สามารถสอบใบรับรองคุณวุฒิของ DPO ได้ ทั้งนี้ ผู้ให้สัมภาษณ์เคยเข้ารับการฝึกอบรมความรู้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของยุโรป แต่ยังไม่มีโอกาสอบรมหลักสูตรกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย เนื่องจากสถานการณ์โควิดที่มีความรุนแรงติดต่อกันมาตั้งแต่ปี 2563”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “ยังไม่มีใบรับรองคุณวุฒิ แต่มีความสนใจหลักสูตรการฝึกบอบรมของหน่วยงานเอกชนและหน่วยงานภาครัฐ เช่น ACIS Professional Center, IMC Institute หลักสูตรของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA: Thailand Digital Government Academy) หลักสูตรของสภาดิจิทัลฯ ที่กำลังดำเนินการพัฒนาหลักสูตรอยู่ในปัจจุบัน”

[39] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “แผนจัดฝึกอบรม Certificate Data Protection Officer (CDPO Thailand) ขององค์กรซึ่งเป็นหลักสูตรเกี่ยวกับการปฏิบัติงานด้านเทคโนโลยีตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานของต่างประเทศโดยตรงนั้น จะถูกเลื่อนออกไปในช่วงปลายปี 2564 เนื่องจากปัญหาโควิด-19 จึงทำให้ยังไม่มีการรับรองคุณวุฒิของ DPO”
- นอกจากนี้ DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งเสริมว่า “DPO และคณะทำงานขององค์กรต้องการหลักสูตรการฝึกอบรมในเชิงลึกมากกว่าหลักสูตรความรู้ทั่วไปที่มีอยู่อย่างแพร่หลายในปัจจุบัน”

4.4 สมาคมหรือชมรมที่เกี่ยวข้อง

เนื่องจากปัจจุบันกฎหมายในส่วนที่เกี่ยวข้องกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลยังอยู่ในช่วงเริ่มต้น จึงยังไม่มีการก่อตั้งสมาคมหรือชมรมที่เกี่ยวข้องโดยตรง ผู้เขียนจึงได้ทำการสัมภาษณ์ DPO และบุคคลที่เกี่ยวข้องของแต่ละสถาบันการเงินว่า “DPO ขององค์กรได้เข้าร่วมเป็นสมาชิกกลุ่มชมรม/สมาคมเกี่ยวกับ DPO ใดบ้าง (ทั้งที่เป็นทางการและไม่เป็นทางการ) และชมรม/สมาคมเหล่านี้มีความเคลื่อนไหวอย่างไรบ้าง”

ตารางที่ 39 ชมรม/สมาคมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ DPO หรือสถาบันการเงินผู้ให้สัมภาษณ์เป็นสมาชิก

ชื่อสมาคม / ชมรม	จำนวนผู้ให้สัมภาษณ์ที่เป็นสมาชิก	ความเป็นมาและความคืบหน้าของสมาคม/ชมรม
1. สมาคมธนาคารไทย	13 แห่ง	สถาบันการเงินสมาชิก (โดยมีคณะผู้จัดทำหลัก คือ ธนาคารพาณิชย์ 5 แห่ง ได้แก่ ธนาคารกรุงเทพ ธนาคารกรุงไทย ธนาคารกสิกรไทย ธนาคารไทยพาณิชย์ และธนาคารทิสโก้) ร่วมกับบริษัทดีล้อย ทู้ช โธมัทสุ ไชยยศ ซึ่งเป็นบริษัทที่ปรึกษา ได้จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร (Guideline on Personal Data Protection for Thai Banks) ฉบับเผยแพร่ ณ วันที่ 28 เมษายน 64 เพื่อใช้

ชื่อสมาคม / ชมรม	จำนวนผู้ให้สัมภาษณ์ที่เป็นสมาชิก	ความเป็นมาและความคืบหน้าของสมาคม/ชมรม
		เป็นข้อเสนอแนะสำหรับธนาคารสมาชิกนำไปพิจารณาเป็นแนวปฏิบัติเบื้องต้นตามที่ธนาคารสมาชิกเห็นสมควรเพื่อรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. DPO-Thailand	5 ท่าน	Line กลุ่มของ DPO จากการสัมมนาของกระทรวงดิจิทัลฯ เป็นกลุ่มชมรมที่ไม่เป็นทางการ ประกอบด้วยผู้ทรงคุณวุฒิหลากหลายที่ของประเทศไทยทั้งภาครัฐและเอกชน ซึ่งแลกเปลี่ยนความรู้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยและของสหภาพยุโรป (GDPR) รวมถึง Framework ที่เกี่ยวข้องอยู่เป็นประจำ แต่เนื่องจากภายหลังมีการประกาศเลื่อนการบังคับใช้กฎหมาย จึงให้ความสำคัญกับการตอบข้อสงสัย แลกเปลี่ยนข่าวสาร และกรณีศึกษาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของแต่ละภาคธุรกิจที่เกิดขึ้นในต่างประเทศเป็นหลัก
3. ชมรมนักกฎหมาย และชมรม Compliance ของสมาคมธนาคารไทย	2 ท่าน	เป็นชมรมภายใต้สมาคมธนาคารไทยที่ตั้งขึ้นเพื่อส่งเสริมความร่วมมือ แลกเปลี่ยนความรู้ ประสบการณ์ รวมทั้งอัพเดทกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เมื่อวันที่ 2 ธันวาคม 63 ได้มีการจัดงานสัมมนาหัวข้อ “แนวปฏิบัติเรื่องบทบาทหน้าที่ของ 2nd and 3rd line เพื่อตอบโจทย์ PDPA & Data breach” โดยในปัจจุบันกำลังเปิดรับฟังความเห็นคิดของผู้เชี่ยวชาญและหน่วยงานภาครัฐเกี่ยวกับการตีความกฎหมายเรื่องต่างๆ เช่น ผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล หรือฐานประโยชน์โดยชอบธรรม (legitimate interest) ครอบคลุมถึงรูปแบบผลิตภัณฑ์และการให้บริการใดของธนาคารบ้าง ตลอดจนการตอบข้อซักถามอื่น เช่น การ

ชื่อสมาคม / ชมรม	จำนวนผู้ให้สัมภาษณ์ที่เป็นสมาชิก	ความเป็นมาและความคืบหน้าของสมาคม/ชมรม
		ขอความยินยอมในการเก็บข้อมูลอ่อนไหว
4. ASEAN Chief Information Officer Association (ACIOA)	2 ท่าน	องค์กรไม่แสวงหาผลกำไร ก่อตั้งขึ้นเมื่อปี พ.ศ. 2557 เพื่อเชื่อมโยงการสื่อสารและแบ่งปันข้อมูลในกลุ่มผู้ใช้เทคโนโลยีสารสนเทศ รวมถึงผู้บริหารฝ่ายข้อมูลของประเทศไทยและต่างประเทศ ภายหลังมีการออกพระราชบัญญัติฯ กลุ่มดังกล่าวจัดสัมมนาและแลกเปลี่ยนความรู้ความคิดเห็นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำ เช่น Clubhouse event “มาทำความเข้าใจกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบริบทของคุณ” เมื่อวันที่ 30 ก.ย. 64 หรือ Thailand PDPA Case study #2 towards the enforcement of PDPA เมื่อวันที่ 27 พ.ค. 64
5. ศูนย์การวิเคราะห์และเผยแพร่ข้อมูลการให้บริการทางการเงิน (Financial Services - Information Sharing and Analysis Center: FS-ISAC)	1 ท่าน	หน่วยงานให้บริการข้อมูลข่าวกรองไซเบอร์ (Cyber Threat Intelligence) เกี่ยวกับลักษณะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นของสถาบันการเงินทั่วโลก เพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงและความยืดหยุ่นของระบบการเงิน รวมถึงนำมาวิเคราะห์เพื่อป้องกันระบบของสถาบันการเงินในประเทศล่วงหน้า เช่น จากรายงานของ FS-ISAC[40] พบการโจมตีจากมัลแวร์เรียกค่าไถ่ Ryuk ในช่วงปี 2562-2563 มากกว่ามัลแวร์ชนิดอื่น โดยเฉพาะองค์กรภาครัฐและองค์กรด้านสาธารณสุขในประเทศสหรัฐอเมริกา เนื่องจากความสามารถในการแพร่กระจายเป็นวงกว้างผ่านทางอีเมล์ของ Trickbot และ Emotet

[40] FS-ISAC, ‘The Rise and Rise of Ransomware’ <https://www.fsisac.com/hubfs/Campaigns/RansomwareReport-2020/FS-ISAC_Ransomware2020.pdf> accessed 28 September 2021.

ชื่อสมาคม / ชมรม	จำนวนผู้ให้สัมภาษณ์ที่เป็นสมาชิก	ความเป็นมาและความคืบหน้าของสมาคม/ชมรม
6. Operational Risk Data Exchange Association (ORX)	1 ท่าน	องค์กรแลกเปลี่ยนข้อมูลความเสี่ยงด้านการปฏิบัติการ มีวัตถุประสงค์เพื่อส่งเสริมความรู้ความเข้าใจทฤษฎี กลยุทธ์ และแนวปฏิบัติเกี่ยวกับความเสี่ยงด้านการปฏิบัติการให้แก่หน่วยงานทางการเงินทั่วโลกที่เป็นเป็นสมาชิก เช่น Banking Operational Risk Loss Data Report 2021, Three Lines of Defence Practice Benchmark เป็นต้น

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากผลการสัมภาษณ์ตามตารางข้างต้น พบว่า[41] สมาคมธนาคารไทย เป็นสมาคมที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพียงแห่งเดียวที่สถาบันการเงินแต่ละแห่งเป็นสมาชิก สำหรับชมรม/สมาคมที่ DPO ของสถาบันการเงินต่างๆ ส่วนใหญ่เป็นสมาชิก ได้แก่ กลุ่มชมรม DPO-Thailand (Line) (5 ท่าน) ชมรมนักกฎหมายและชมรม Compliance ของสมาคมธนาคารไทย (2 ท่าน) ASEAN Chief Information Officer Association (ACIOA) (2 ท่าน) ศูนย์การวิเคราะห์และเผยแพร่ข้อมูลการให้บริการทางการเงิน (FS-ISAC) (1 ท่าน) และ Operational Risk Data Exchange Association (ORX) (1 ท่าน)

4.5 การจัดฝึกอบรมความรู้ภายในสถาบันการเงิน

กฎหมายกำหนดให้สถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่สนับสนุนการปฏิบัติหน้าที่ของ DPO โดยให้ DPO ได้รับการฝึกอบรมเพื่อรักษาไว้ซึ่งความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูล[42] ซึ่งสถาบันการเงินสนับสนุนให้ DPO เข้ารับการฝึกอบรมของหน่วยงานภายนอกหรือเป็นการจัดฝึกอบรมภายในองค์กรก็ได้

[41] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[42] GDPR, Article 38(2)

ดังที่ได้กล่าวถึงใน “หัวข้อ 3.2.3 การเข้ารับการฝึกอบรม” ว่าการฝึกอบรมความรู้ความเข้าใจกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นทรัพยากรที่ผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลภายในสถาบันการเงินต้องการมากเป็นอันดับสาม ผู้เขียนได้การทำสัมภาษณ์ต่อไปว่า “สถาบันการเงินแต่ละแห่งมีการจัดฝึกบอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลมาแล้วกี่ครั้ง ให้กับบุคคลในระดับใดบ้าง”

ผลการสัมภาษณ์พบว่า[43] ตั้งแต่ช่วงปี 2562 ถึงปี 2564 สถาบันการเงินต่างๆ ให้ความสำคัญกับการฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่พนักงานภายในองค์กรเป็นอย่างมาก โดยผลการสัมภาษณ์พบว่าสถาบันการเงินในประเทศไทยแต่ละแห่งได้มีการจัดฝึกอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรภายในองค์กรมาแล้วโดยเฉลี่ย 16 ครั้ง สูงสุด 70 ครั้ง และต่ำสุด 3 ครั้ง ซึ่งมีทั้งรูปแบบของการฝึกอบรมออนไลน์ (Online course) การทำเวิร์คช็อป (Workshop) และการสื่อสารในรูปแบบอินโฟกราฟิก (Infographic) ซึ่งมีความแตกต่างกันไปขึ้นอยู่กับความพร้อมของแต่ละสถาบันการเงิน ให้แก่พนักงานในระดับผู้บริหารไปจนถึงระดับพนักงานทั่วไป โดยความเข้มข้นของเนื้อหาการจัดฝึกอบรมจะขึ้นอยู่กับลักษณะการปฏิบัติงานหรือบทบาทหน้าที่ของผู้ที่จะเข้ารับการฝึกอบรม เช่น การกรอกรายการกิจกรรมการประมวลผลข้อมูล (ROPA) และแบบฟอร์มต่างๆ ให้แก่ตัวแทนด้านการคุ้มครองข้อมูลส่วนบุคคลประจำฝ่ายงานและผู้ช่วย หรือเน้นการฝึกอบรมเกี่ยวกับการขอความยินยอมของลูกค้าให้แก่พนักงานบริการลูกค้า (Front Office) เป็นต้น นอกจากนี้ สถาบันการเงินบางแห่งยังมีการจัดฝึกอบรมให้แก่บริษัทในเครือรวมถึงคู่ค้า (Vendor)

อย่างไรก็ดี DPO ของสถาบันการเงิน 3 แห่ง มีความเห็นไปในทางเดียวกันว่า เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายใหม่และมีลักษณะที่ค่อนข้างเป็น ‘กฎหมายเทคนิค’ ฉะนั้น ผู้ที่มีความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างลึกซึ้งในประเทศไทยจึงหายาก โดยเฉพาะอย่างยิ่งในแวดวงสถาบันการเงินยิ่งมีจำนวนน้อยมาก นอกจากนี้ DPO ของสถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่งยังมีแนวความเห็นว่า หลักสูตรส่วนใหญ่ที่มีอยู่ในปัจจุบันมักเป็นหลักสูตรพื้นฐานหรือความรู้ทั่วไป ผู้ปฏิบัติงานในคณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินแต่ละแห่งต้องการหลักสูตรขั้นสูงกว่านั้น[44]

[43] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[44] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

4.6 ความคืบหน้าทางกฎหมายเกี่ยวกับการรับรองคุณสมบัติของ DPO และการรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

ในส่วนนี้ผู้เขียนจะกล่าวถึงความเคลื่อนไหวของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งเป็นหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลขององค์กรต่างๆ และความเคลื่อนไหวของสถาบันคุณวุฒิวิชาชีพ เกี่ยวกับการจัดทำร่างกฎหมายเกี่ยวกับการรับรองคุณสมบัติของ DPO และการรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

4.6.1 การรับรองคุณสมบัติของ DPO

ทางปฏิบัติบุคคลที่จะเข้ามาดำรงตำแหน่ง DPO อาจมีใบรับรองคุณวุฒิซึ่งแสดงให้เห็นว่าตนผ่านการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลมาแล้วเป็นจำนวนมากและมีความรู้ความสามารถมากเพียงพอต่อการปฏิบัติหน้าที่ในตำแหน่ง DPO ขององค์กร แต่องค์กรจะต้องพิจารณาถึงความถูกต้องและความน่าเชื่อถือของการฝึกอบรมหรือใบรับรองคุณวุฒิเหล่านั้น[45] เช่น แท้จริงแล้วบุคคลที่ต้องการสมัครเป็น DPO ขององค์กรผ่านการฝึกอบรมที่จัดขึ้นเพียงวันเดียว หรือได้ใบรับรองคุณวุฒิมาเพียงเพราะลงทะเบียนเสียค่าสมัครเรียน หรือเป็นการสอบวัดระดับความรู้แบบง่ายๆ ขาดเกณฑ์การวัดผลความรู้ความเข้าใจที่เหมาะสม ทำให้บุคคลเหล่านั้นมีความสามารถไม่เพียงพอต่อตำแหน่ง DPO ที่จะต้องมีความรู้ความเข้าใจอยู่ในระดับที่เชี่ยวชาญ

ประเด็นทางกฎหมายเกี่ยวกับการรับรองคุณสมบัติของ DPO ในประเทศไทยนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41 วรรคหก กำหนดว่า “คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล” โดยความคืบหน้าในปัจจุบันนั้นปรากฏว่าในขณะที่ยังไม่มีการประกาศกำหนดคุณสมบัติของ DPO อย่างเป็นทางการ สำนักงานคณะกรรมการคุ้มครอง

[45] ผู้เขียนเรียบเรียงจาก Eric Lachaud, "DPO certification should be monitored," SSRN Electric Journal.

ข้อมูลส่วนบุคคลได้ว่าจ้างที่ปรึกษาเพื่อศึกษาการจัดทำร่างกฎหมายลำดับรอง ซึ่งมีข้อเสนอเรื่องการกำหนดคุณสมบัติเป็นการทั่วไป ไม่เฉพาะเจาะจงตามอุตสาหกรรม[46] ดังนี้

"DPO จะต้องเป็นบุคคลธรรมดาที่มีความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการอาจประกาศรับรองหลักสูตรซึ่งจัดโดยสำนักงานหรือหน่วยงานที่ได้รับการรับรองอื่นอันเป็นหลักสูตรอบรมทักษะและความเชี่ยวชาญซึ่งจำเป็นต่อการปฏิบัติหน้าที่ของ DPO ได้ และกำหนดให้ DPO ต้องได้รับการอบรมหรือผ่านการทดสอบจากหลักสูตรดังกล่าวก็ได้ เมื่อคณะกรรมการประกาศรับรองหลักสูตรแล้ว ผู้ที่จะได้รับการแต่งตั้งเป็น DPO ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับการอบรมหรือจะต้องผ่านการทดสอบจากหลักสูตรดังกล่าว ทั้งนี้ ต้องได้รับการอบรมหรือผ่านการทดสอบไม่เกิน 1 ปี ขณะแต่งตั้งระหว่างการดำรงตำแหน่ง DPO นอกจากนี้ DPO จะต้องได้รับการอบรมหรือผ่านการทดสอบจากหลักสูตรซึ่งคณะกรรมการรับรองเพื่อพัฒนาทักษะและความรู้อย่างสม่ำเสมออย่างน้อยทุก 3 ปี หลักเกณฑ์และวิธีการรับรองหลักสูตร รวมถึงข้อกำหนดอื่นใดเกี่ยวกับสถาบันผู้ดำเนินหลักสูตร ให้เป็นไปตามประกาศคณะกรรมการที่เกี่ยวข้อง..."[47]

ในระหว่างนี้ สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) อยู่ระหว่างจัดทำร่างมาตรฐานอาชีพและคุณวุฒิวิชาชีพสาขาอุตสาหกรรมดิจิทัล โดยกำหนดให้อาชีพนักจัดการคุ้มครองข้อมูลส่วนบุคคล แบ่งทักษะเป็นระดับปฏิบัติการ บริหารและเชี่ยวชาญ ทั้งนี้ ผู้ที่จะทำหน้าที่เป็น DPO ต้องได้รับการประเมินว่ามีทักษะในระดับเชี่ยวชาญ[48] ดังต่อไปนี้[49]

---

[46] ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, "สัมภาษณ์ เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล." 29 กรกฎาคม 2564.

[47] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.9 "ให้ถือว่า DPO ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้แต่งตั้งขึ้นขณะที่ยังไม่มีประกาศของคณะกรรมการฯ มีคุณสมบัติครบถ้วนตามที่กำหนดแล้ว และให้ถือว่าได้รับการอบรมหรือผ่านการทดสอบเพื่อพัฒนาทักษะและความรู้อย่างสม่ำเสมอแล้ว". โปรดดู https://www.law.chula.ac.th/event/10941/

[48] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

[49] สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน), มาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขา Digital security and privacy (2564), หน้า.31-32.

1. มีประสบการณ์การทำงานด้านข้อมูลสารสนเทศในองค์กรอย่างน้อย 5 ปี หรือมีหลักฐานการผ่านการอบรมหลักสูตรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
2. ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล[50]
3. การต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เป็นไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ (Assessment Standard)

อย่างไรก็ตาม การจัดทำมาตรฐานอาชีพข้างต้นเป็นเพียงการกำหนดกรอบคุณวุฒิแต่ละระดับตามสมรรถนะ (Competency) ส่วนการจัดทำหลักสูตรเพื่อให้ผู้เข้าร่วมการอบรมมีองค์ความรู้และทักษะที่จะผ่านการประเมินได้นั้น เป็นการดำเนินงานขององค์กรที่จัดฝึกอบรม[51]

4.6.2 การรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

ดังที่ได้กล่าวไว้ในตอนต้นของ “หัวข้อ 4.6.1 การรับรองคุณสมบัติของ DPO” ว่าใบรับรองคุณวุฒิของบุคคลที่ต้องการเข้ามาเป็น DPO ขององค์กรไม่ใช่หลักฐานที่แสดงให้เห็นว่าบุคคลคนนั้นมีความรู้ความสามารถเพียงพอต่อการปฏิบัติหน้าที่ สถาบันการเงินจึงมิอาจพิจารณาแต่งตั้งบุคคลใดภายนอกองค์กรเป็น DPO เพียงเพราะใบรับรองคุณวุฒิได้ แต่บุคคลดังกล่าวจะต้องผ่านหลักสูตรการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

สำหรับความคืบหน้าของกฎหมายไทยเกี่ยวกับการรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลนั้น ปัจจุบันมีร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง

---

[50] สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน), ร่างมาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขา Digital security and privacy (2564), หน้า.31-32. (หน่วยสมรรถนะ หรือ Unit of Competency ของอาชีพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ได้แก่ การให้คำปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคล การบริหารจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล การบริหารจัดการเหตุละเมิดข้อมูลส่วนบุคคล การดำเนินการจัดทำนโยบายและแนวปฏิบัติ การบริหารจัดการผู้มีส่วนได้ส่วนเสีย การส่งและโอนข้อมูล ธรรมภิบาลข้อมูลและหลักจริยธรรม และการตรวจสอบการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล)

[51] ดร.สุนทรีย์ ส่งเสริม, เรื่องเดิม

มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล ซึ่งตามร่างประกาศฯ ดังกล่าว ผู้มีสิทธิ (องค์กรจัดฝึกอบรม) ที่จะยื่นขอรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามที่สำนักงานฯ มอบหมายนั้น ต้องเป็นบุคคลใดบุคคลหนึ่ง ดังต่อไปนี้[52]

- สถาบันการศึกษา
- สถาบันวิจัย
- สถาบันหรือหน่วยงานของรัฐที่มีวัตถุประสงค์เพื่อจัดฝึกอบรม
- บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่มีหน่วยฝึกอบรมภายใน
- บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่มีวัตถุประสงค์เพื่อจัดฝึกอบรมหรือพัฒนาบุคลากร

โดยหลักสูตรของหน่วยงานฝึกอบรมที่จะผ่านการรับรองตามเกณฑ์ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ต้องเป็นหลักสูตรที่ครอบคลุมความรู้พื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคล และมาตรฐานทางอุตสาหกรรม (ISO) ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเป้าหมายของหลักสูตร โดยหลักสูตรดังกล่าวต้องมีวิธีการประเมินผลภายหลังจากการฝึกอบรมอย่างมีระบบ รวมถึงหลักสูตรฝึกอบรมนั้นจะต้องมีวิทยากรที่มีความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล[53]

ทั้งนี้ ดังที่เคยกล่าวใน “หัวข้อ 4.5 การจัดฝึกอบรมความรู้ภายในสถาบันการเงิน” ผู้ให้สัมภาษณ์ของสถาบันการเงินหลายรายมีแนวความเห็นว่า “หลักสูตรส่วนใหญ่ที่มีอยู่ในปัจจุบันมักเป็นหลักสูตรพื้นฐานหรือความรู้ทั่วไป ผู้ปฏิบัติงานในคณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินแต่ละแห่งต้องการหลักสูตรขั้นสูงกว่านั้น”[54] ผู้เขียนเห็นว่าการที่ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วน

---

[52] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล หมวด 3 ข้อ 2.24. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

[53] ibid. หมวด 3 ข้อ 2.25. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

[54] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

บุคคล กำหนดความรู้ความเข้าใจในด้านต่างๆ อันเป็นองค์ประกอบของหลักสูตรการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลดังที่กล่าวข้างต้น เป็นเพียงความรู้ความเข้าใจขั้นต่ำสำหรับตำแหน่งผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระดับทั่วไปเท่านั้น ทั้งยังไม่มีลักษณะเฉพาะเจาะจงกับธุรกิจสถาบันการเงิน

ผู้เขียนมีความเห็นว่าตำแหน่ง DPO ของสถาบันการเงินจำเป็นจำเป็นมีความรู้ความเข้าใจใน 3 ด้านนี้อย่างถ่องแท้ ได้แก่ (1) กฎหมาย (2) แนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ และ (3) รูปแบบการดำเนินธุรกิจและการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงิน โดยความรู้ความเข้าใจในอีก 2 ด้านต่อไปนี้จะส่งเสริมให้การปฏิบัติหน้าที่ DPO ตามกฎหมายนั้นสัมฤทธิ์ผลมากขึ้น ได้แก่ (1) การบริหารจัดการความเสี่ยง และ (2) มาตรฐานความปลอดภัยของข้อมูลส่วนบุคคล เช่น GDPR, ISO/IEC 27001 (ISMS), ISO/IEC 27701 (PIMS), NIST Privacy Framework

บทที่ 5

ปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงิน

เมื่อ DPO ของสถาบันการเงินทำหน้าที่ให้คำแนะนำและตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กรให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม จะก่อให้เกิดประโยชน์ทั้งในแง่ของการปฏิบัติตามกฎหมาย และประโยชน์ในแง่ของภาพลักษณ์ธุรกิจขององค์กร กล่าวคือ หากสามารถกำกับดูแลให้การประมวลผลของสถาบันการเงินเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง ย่อมเป็นการสร้างความน่าเชื่อถือและความไว้วางใจแก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ยังทำให้เกิดแนวปฏิบัติที่ดีในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลแก่ภาคธุรกิจหรือองค์กรอื่นๆ ในประเทศไทยโดยรวม

ปัจจุบันสถาบันการเงินต่างๆ ได้มีการจัดทำนโยบาย แนวปฏิบัติ และคู่มือการทำงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละเรื่องภายในองค์กรแล้ว ซึ่งในการจัดทำนโยบาย แนวปฏิบัติและคู่มือการทำงานเหล่านั้นยึดหลักเกณฑ์มาจากแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลของหน่วยงานในประเทศไทย ได้แก่ แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสมาคมธนาคารไทย แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยต่างๆ ในประเทศไทย รวมถึงแนวปฏิบัติของต่างประเทศ และนำมาปรับใช้ให้เหมาะสมกับสภาพการดำเนินธุรกิจในสถาบันการเงินของตน ทั้งนี้ เพื่อให้การประกอบธุรกิจขององค์กรมีความสอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยและมาตรฐานสากล โดยแนวปฏิบัติและคู่มือการทำงานของสถาบันการเงินส่วนใหญ่มักประกอบด้วยเรื่องต่างๆ ได้แก่ การกำหนดและแยกแยะข้อมูลส่วนบุคคล (Data Classification) หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล การทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ฐานการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) การขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคล การใช้และเปิดเผยข้อมูลส่วนบุคคล การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ การเก็บรักษาและลบข้อมูลส่วนบุคคล การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล การทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) การจัดการเหตุละเมิดข้อมูลส่วนบุคคล นอกจากนี้ ยังมีการจัดทำมาตรฐานและแนวปฏิบัติ

เกี่ยวกับการกำกับดูแลข้อมูล เช่น มาตรการรักษาความมั่นคงปลอดภัยด้านข้อมูล (Data Security Measures) และแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล (Data Labeling Guideline)[1] ซึ่งมาตรฐานและแนวปฏิบัติเหล่านี้ล้วนมีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วย

ในการให้คำปรึกษาหารือและดูแลตรวจสอบของ DPO เพื่อให้นโยบาย แนวปฏิบัติ หรือคู่มือการทำงานภายในองค์กร รวมถึงกระบวนการประมวลผลข้อมูลส่วนบุคคลของแต่ละสถาบันการเงินเป็นไปตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล DPO จะต้องคำนึงถึงข้อพิจารณาในส่วนที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างน้อยตามรายการ ดังต่อไปนี้[2]

1. การประมวลผลข้อมูลมีความชอบด้วยกฎหมายเป็นไปตามมาตรา 24 และมาตรา 26 แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Lawful Basis)
2. มีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลและประกาศให้เจ้าของข้อมูลส่วนบุคคลทราบ รวมถึงแจ้งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลที่ครบถ้วนตามมาตรา 23 หรือมาตรา 25 แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Privacy Policy/Privacy Notice)
3. มีการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 ถึงมาตรา 36 แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Data Subject Rights)
4. มีการกำหนดระยะเวลาในการจัดเก็บข้อมูลและมาตรการในการลบหรือทำลายข้อมูลตามมาตรา 37 (3) แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Data Retention and Data Disposal)
5. มีกระบวนการรองรับเพื่อแจ้งเหตุละเมิดข้อมูลตามมาตรา 37(4) แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Data Breach Notification)

---

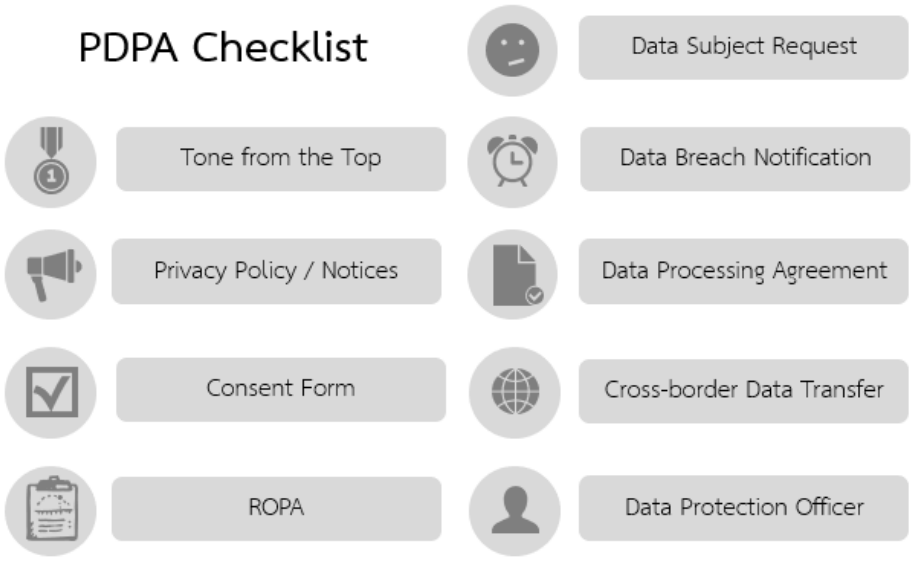
[1] ผู้เขียนเรียบเรียงจาก บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง , เรื่องเดิม

[2] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล หมวด 3 ข้อ 2.5. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

6. มีการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่เป็นการประมวลผลที่ใช้เทคโนโลยีใหม่หรือมีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล และประกาศคณะกรรมการที่เกี่ยวข้อง (Data Protection Impact Assessment)
7. มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (DPO)
8. มีการโอนข้อมูลไปยังต่างประเทศที่ชอบด้วยกฎหมายตามมาตรา 28 ถึงมาตรา 29 แห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Cross-border Data Transfer)
9. กรณีที่มีการประมวลผลโดยผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องมีการทำข้อตกลงประมวลผลข้อมูลส่วนบุคคลตามมาตรา 40 วรรคสามแห่งพระราชบัญญัติฯ และประกาศคณะกรรมการที่เกี่ยวข้อง (Data Processing Agreement)

ตามมาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคลข้างต้น สามารถสรุปรายการข้อพิจารณาการตรวจสอบกระบวนการคุ้มครองข้อมูลส่วนบุคคลขององค์กรได้ ดังภาพด้านล่างนี้

ภาพที่ 9 ข้อพิจารณาการตรวจสอบองค์กรให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล



ที่มา: ปิยะบุตร บุญอร่ามเรือง, สไลด์ประกอบการบรรยาย Thailand Data Protection Guidelines 3.0 – Business Functions

อย่างไรก็ดี เนื่องจากสภาพความไม่ชัดเจน และความเคร่งครัดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อาจทำให้สถาบันการเงินต่างๆ เกิดปัญหาในการดำเนินการให้เป็นไปตามกฎหมายหลายประการ ดังจะเห็นได้จาก การมีประกาศเลื่อนการบังคับใช้กฎหมายออกไปเป็นวันที่ 1 มิถุนายน พ.ศ. 2565 เพราะการปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดนั้น มีรายละเอียดมากและซับซ้อน และต้องใช้เทคโนโลยีขั้นสูงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ ประกอบกับสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ยังคงมีอยู่อย่างต่อเนื่องและรุนแรงยิ่งขึ้นจนถึงปัจจุบัน ส่งผลกระทบต่อเศรษฐกิจและสังคมโดยรวมเป็นอย่างมาก[3] ทำให้สถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงหน่วยงานและกิจการต่างๆ จำนวนมากทั่วประเทศยังไม่พร้อมที่จะปฏิบัติตามพระราชบัญญัติดังกล่าว

สำหรับเนื้อหาของบทที่ 5 นี้ ผู้เขียนจะทำการศึกษาปัญหาที่เกิดจากการดำเนินการให้เป็นไปตามกฎมายคุ้มครองข้อมูลส่วนบุคคล (PDPA Implementation) ของสถาบันการเงิน ซึ่งปัญหาดังกล่าวเป็นปัญหาทางปฏิบัติของผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร รวมถึงเป็นปัญหาของ DPO ด้วยในขณะเดียวกัน

โดยผู้เขียนได้กำหนดแนวทางการศึกษาและทำการเก็บข้อมูล จากการสัมภาษณ์ DPO และบุคคลในคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินต่างๆ ในประเทศไทย จำนวน 13 แห่ง (ซึ่งประกอบด้วยสถาบันการเงินดังที่กล่าวไว้ในตอนต้นของบทที่ 3) ซึ่งมีคำถามที่ใช้ในการสัมภาษณ์ คือ สถาบันการเงินพบปัญหาใดในการดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลบ้าง เช่น การสนับสนุนจากผู้บริหารระดับสูง (Tone from the Top) การประกาศแจ้งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) การเก็บรักษาและลบข้อมูลส่วนบุคคล (Data Retention) การจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) หรือ การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer) โดยให้ผู้ให้สัมภาษณ์กล่าวถึงรายละเอียดของปัญหาที่พบเหล่านั้น

[3] พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564

หากผู้ให้สัมภาษณ์ระบุถึงปัญหามากกว่า 1 ปัญหา จะให้ผู้ให้สัมภาษณ์เรียงลำดับปัญหาที่เห็นว่าต้องให้ความสำคัญเร่งด่วนมากที่สุดไปยังน้อยที่สุด

จากแบบสอบถามและการสัมภาษณ์พบว่า[4] ปัญหาที่เกิดขึ้นจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินต่าง โดยปัญหาแต่ละอย่างที่ผู้ให้สัมภาษณ์กล่าวถึงและทำการประเมินอันดับความสำคัญหรือความจำเป็นเร่งด่วน (ทั้งนี้ เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยยังอยู่ในขั้นเริ่มต้นจึงทำให้ผู้ให้สัมภาษณ์อาจขาดความเข้าใจในการปฏิบัติงานตามกฎหมาย ประกอบกับผู้ให้สัมภาษณ์ของสถาบันการเงินแต่ละแห่งมีเวลาให้สัมภาษณ์ที่จำกัด ปัญหาที่เกิดขึ้นจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะระบุต่อไปจึงไม่ครบถ้วนทุกด้านได้) ปรากฏตามตารางดังต่อไปนี้

ตารางที่ 40 ปัญหาที่เกิดขึ้นจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินที่ผู้ให้สัมภาษณ์กล่าวถึง

ปัญหาที่เกิดขึ้น	ขนาดใหญ่	ขนาดกลาง	ขนาดเล็ก
การเก็บรักษา ลบ และการทำข้อมูลส่วนบุคคลนิรนาม (Data Retention, Disposal, Anonymization)	4	1	4
บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)	4	-	3
การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification)	5	-	2
การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request - DSR)	2	-	3
แบบฟอร์มขอความยินยอม (Consent Form)	2	-	2
การโอนข้อมูลส่วนบุคคลไปต่างประเทศ/องค์การระหว่างประเทศ (Cross-border Data Transfer)	-	-	2
ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice)	1	-	1
ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (DPA)	2	-	1

[4] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ตารางที่ 41 อันดับปัญหาที่เกิดขึ้นจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินที่ผู้ให้สัมภาษณ์ทำการประเมิน

อันดับความสำคัญ	ขนาดใหญ่ (แห่ง)	ขนาดกลาง (แห่ง)	ขนาดเล็ก (แห่ง)
1	ROPA (4)	เก็บรักษา-ลบข้อมูล (1)	เก็บรักษา-ลบข้อมูล (1) แบบขอความยินยอม (1) โอนข้อมูลต่างประเทศ (1) Privacy Notice (1)
2	เก็บรักษา-ลบข้อมูล (3) แบบขอความยินยอม (1)	แบบขอความยินยอม (1)	เก็บรักษา-ลบข้อมูล (1) ROPA (2) คำขอใช้สิทธิฯ (2)
3	แจ้งเหตุละเมิด (2) คำขอใช้สิทธิฯ (2)	-	แจ้งเหตุละเมิด (1) คำขอใช้สิทธิฯ (1)
4	เก็บรักษา-ลบข้อมูล (1) แจ้งเหตุละเมิด (2) ข้อตกลงประมวลผล (1)	-	เก็บรักษา-ลบข้อมูล (1) แจ้งเหตุละเมิด (1) ข้อตกลงประมวลผล (1)
5	แจ้งเหตุละเมิด (1) ข้อตกลงประมวลผล (1)	-	เก็บรักษา-ลบข้อมูล (1) ROPA (1)
6	Privacy Notice (1)	-	โอนข้อมูลต่างประเทศ (1)
7	แบบขอความยินยอม (1)	-	-
8	-	-	-

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

ในส่วนถัดไป ผู้เขียนจะกล่าวถึงประเด็นต่างๆ ได้แก่ (1) อันดับความสำคัญของแต่ละปัญหา (2) กฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับแต่ละประเด็นปัญหา และ (3) ระบุถึงปัญหาที่เกิดขึ้นจริงกับ DPO และบุคลากรอื่นๆ ที่อยู่ในคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงิน

5.1 การเก็บรักษาและการลบข้อมูลส่วนบุคคล

ผลการสัมภาษณ์พบว่า[5] ปัญหาการเก็บรักษา ลบ และทำข้อมูลส่วนบุคคลนิรนาม (Data Retention, Disposal and Anonymization) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 9 แห่ง กล่าวถึง (ขนาดใหญ่ 4 แห่ง ขนาดกลาง 1 แห่ง และขนาดเล็ก 4 แห่ง) ซึ่งสถาบันการเงินขนาดกลาง 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดใหญ่ 3 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสอง สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสี่ สถาบันการเงินขนาดเล็กอีก 1 แห่งให้ความสำคัญเป็นอันดับห้า ด้วยเหตุนี้ผู้เขียนจึงจัดให้ปัญหาการเก็บรักษา ลบ และทำข้อมูลส่วนบุคคลนิรนาม เป็นปัญหาที่มีสำคัญเป็น *'อันดับแรก'*

โดยหลักเรื่องการเก็บรักษาข้อมูล (Data Retention) ผู้ควบคุมข้อมูลส่วนบุคคลจะจัดเก็บได้เท่าที่ข้อมูลยังมีความเกี่ยวข้องและจำเป็นต่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูล และจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกาหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น[6] ผู้ควบคุมข้อมูลจึงต้องกำหนดนโยบายกำหนดระยะเวลาการเก็บรักษาข้อมูลตามกรอบวัตถุประสงค์ต่างๆ ให้เหมาะสม โดยคำนึงถึงลักษณะภารกิจขององค์กรรวมถึงความจำเป็นและวัตถุประสงค์ของการประมวลผลข้อมูล ส่วนการกำหนดระยะเวลาอาจอ้างอิงตามมาตรฐานการจัดเก็บของอุตสาหกรรมหรือข้อกำหนดตามกฎหมายที่เกี่ยวข้องได้[7] ส่วนในกรณีที่ไม่มีข้อกำหนดและไม่ชัดเจนว่าควรจะเก็บถึงเมื่อใด อาจพิจารณาระบบการเตือนเพื่อให้ฝ่ายที่เกี่ยวข้องพิจารณาความจำเป็นของข้อมูลเป็นระยะๆ

ในบริบทของสถาบันการเงินที่มีการจัดเก็บหรือประมวลผลข้อมูลเป็นจำนวนมาก การปฏิบัติตามข้อกำหนดต่างๆ ตามหลักการใช้ข้อมูลน้อยที่สุดเท่าที่จำเป็น (Data Minimization) ทั้งด้าน

---

[5] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

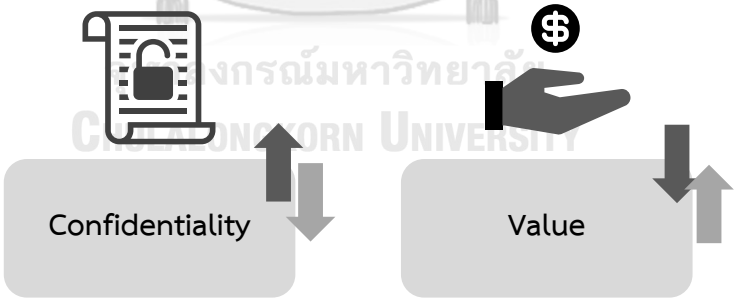
[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1) และ (3)

[7] ตัวอย่างเช่น พ.ร.บ. ปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 22 และ 22/1 กำหนดให้สถาบันการเงินมีหน้าที่ในการจัดเก็บข้อมูลรายละเอียดเกี่ยวกับการแสดงตน (KYC) เป็นเวลา 5 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้า และการเก็บรักษาข้อมูลเกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD) เป็นเวลา 10 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้า

เนื้อหาและระยะเวลาจัดเก็บเป็นเรื่องที่ท้าทายในทางปฏิบัติเป็นอย่างมาก สถาบันการเงินจะต้องเริ่มตั้งแต่การออกแบบระบบจัดการข้อมูลที่ดี แบ่งหมวดหมู่ชนิดข้อมูล บันทึกที่มา หากวัตถุประสงค์การประมวลผลเกี่ยวข้องกับการนำไปประกอบการตัดสินใจควรมีการกำหนดระยะเวลาเพื่ออัพเดทข้อมูลสม่ำเสมอ จัดทำแผนผังการไหลเวียนของข้อมูลภายในองค์กร เพื่อให้การเข้าถึงข้อมูลที่ต้องการเป็นไปได้อย่างรวดเร็ว อย่างไรก็ดี ผู้เขียนคาดว่าการดำเนินงานตามแนวทางข้างต้นน่าจะเป็นภาระงานที่ยากลำบากต่อองค์กรโดยเฉพาะอย่างยิ่งในธุรกิจสถาบันการเงิน เนื่องจากสถาบันการหลายแห่งได้มีการก่อตั้งมาแล้วเป็นระยะเวลานาน ประกอบกับความกระจัดกระจายไม่เป็นระเบียบของข้อมูลจำนวนมากที่ถูกจัดเก็บอยู่ในหลายส่วนงาน

นอกจากนี้ สถาบันการเงินอาจการพัฒนาระบบสารสนเทศเพื่อนำมาใช้ในการประมวลผลข้อมูลส่วนบุคคล โดยดำเนินการตามหลักการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การออกแบบและค่าเริ่มต้น (Data Protection by Design and by Default) เพื่อช่วยลดผลกระทบ ความเสี่ยงที่จะเกิดความเสียหายต่อเจ้าของข้อมูล เช่น การนำมาตรการทางเทคนิคมาประยุกต์ใช้หรือหรือนำเครื่องมือ/เทคโนโลยีสารสนเทศมาสนับสนุน เช่น ทำข้อมูลนิรนาม (Anonymization) เพื่อขจัดความสามารถในการระบุตัวตนของเจ้าของข้อมูลได้ ซึ่งทางกฎหมายจะไม่ถือว่าเป็นข้อมูลส่วนบุคคลอีก[8]

ภาพที่ 10 ความสัมพันธ์ระหว่างการรักษาความลับกับการใช้ประโยชน์ของข้อมูล



กระบวนการทำข้อมูลนิรนามนั้นโดยหลักการแล้วเป็นการชั่งน้ำหนักระหว่างคุณค่าของ (1) การใช้ประโยชน์ของข้อมูล (Value) กับ (2) การรักษาความลับของเจ้าของข้อมูล (Confidentiality) หากผู้ที่จัดทำข้อมูลนิรนามสามารถแสดงให้เห็นว่าได้ดำเนินการตามสมควรในการรักษาความลับของเจ้าของข้อมูลนั้น โดยไม่สูงเกินไปกว่าคุณค่าจากการใช้ประโยชน์ของข้อมูล (value) ดังกล่าวแล้ว ก็

[8] สมาคมธนาคารไทย, แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร สมาคมธนาคารไทย (Guideline on Personal Data Protection for Thai Banks) (2564), หน้า.71-72.

ย่อมถือว่ามีการจัดทำข้อมูลนิรนามในระดับที่เหมาะสม ในขณะเดียวกันการจัดทำข้อมูลนิรนามนั้นแม้จะเพิ่มการรักษาความลับ แต่ในขณะเดียวกันก็จะลดคุณค่าของข้อมูลด้วยเช่นกัน

ในส่วนถัดไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติที่เกิดขึ้นเกี่ยวกับการเก็บรักษาและการลบ รวมถึง การทำข้อมูลส่วนบุคคลนิรนามของสถาบันการเงินผู้ให้สัมภาษณ์ จำนวน 9 แห่ง ข้างต้น

ภาพที่ 11 ปัญหาทางปฏิบัติการเก็บรักษาและลบข้อมูลส่วนบุคคล (Data Retention & Disposal)

- ❖ เนื่องจากข้อมูลชุดใดชุดหนึ่งถูกใช้โดยหลายฝ่ายงานและอยู่ภายใต้หลายระบบจัดการข้อมูล จึงยากต่อการกำหนดแนวปฏิบัติเรื่องระยะเวลาการเก็บ ลบ ทำลายข้อมูลส่วนบุคคลภายในสถาบันการเงิน
- ❖ การลบหรือทำลายข้อมูลส่วนบุคคลครบทั้งวงจร มีความยุ่งยาก ใช้เวลาดำเนินการนาน
- ❖ สถาบันการเงินขาดระบบค้นหาและติดตามข้อมูลส่วนบุคคล ทำให้ไม่ทราบว่ากระจัดกระจายอยู่ที่ใดบ้าง จึงไม่สามารถลบหรือทำลายข้อมูลที่หมดความจำเป็นได้อย่างครบถ้วน
- ❖ บางครั้งไม่สามารถลบตามคำขอของ Data Subject ได้ เพราะข้อมูลนั้นเป็น Primary Key
- ❖ ข้อมูลอาจถูกสำรองอยู่นอกระบบ เช่น แล็ปท็อป คลาวด์ส่วนตัวของพนักงาน
- ❖ การลงทุนจัดทำข้อมูลนิรนาม (Data Anonymization) เสียค่าใช้จ่ายเป็นจำนวนมาก และมีความยุ่งยาก เพราะความกระจัดกระจายของข้อมูล

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

สำหรับปัญหาทางปฏิบัติที่เกิดขึ้นเกี่ยวกับการเก็บรักษาและการลบข้อมูลส่วนบุคคลของสถาบันการเงินในประเทศไทยนั้น จากการสัมภาษณ์พบว่า[9] เนื่องจากกระบวนการทำงานของแต่ละฝ่ายงานภายในสถาบันการเงินมีความแตกต่างกัน ในบางกรณี ข้อมูลชุดเดียวกันถูกใช้งานจากหลากหลายฝ่ายงาน และหลากหลายระบบจัดการข้อมูล ทำให้ยากต่อการกำหนดมาตรฐานระยะเวลาในการเก็บรักษาและการทำลายข้อมูลส่วนบุคคลของสถาบันการเงิน โดย DPO ของสถาบันการเงินแห่งหนึ่ง กล่าวว่า “ต้องการแนวปฏิบัติเกี่ยวกับระยะเวลาจัดเก็บข้อมูล (เช่น สถาบันการเงินสามารถจะเก็บข้อมูลสินเชื่อหรือข้อมูลทางการตลาดได้นานเท่าใด) และแนวปฏิบัติเกี่ยวกับวิธีลบข้อมูลส่วนบุคคลซึ่งกระจัดกระจายอยู่หลากหลายที่ภายในองค์กร”

อีกประเด็นปัญหาหนึ่ง คือ ปัญหาทางเทคนิคในการลบข้อมูลส่วนบุคคลที่หมดความจำเป็นแล้ว ซึ่งเป็นประเด็นที่ถูกกล่าวถึงโดยสถาบันการเงินมากถึง 7 แห่งจาก 9 แห่ง สถาบันการเงินเหล่านี้

[9] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

กล่าวว่า[10] การลบหรือทำลายข้อมูลส่วนบุคคลให้ครบทั้งวงจรมีความยุ่งยากต่อการปฏิบัติและใช้ระยะเวลามากในการดำเนินการ ยิ่งไปกว่านั้นข้อเท็จจริงปรากฏว่าไม่สามารถลบหรือทำลายข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ภายในองค์กรเมื่อหมดความจำเป็นในการใช้งานออกไปได้ทั้งหมด เพราะสถาบันการเงินขาดระบบค้นหาว่าข้อมูลส่วนบุคคลถูกจัดเก็บไว้ในรูปแบบใดและอยู่ในหน่วยงานใดภายในองค์กรและข้อมูลบางอย่างไม่สามารถลบหรือทำลายในทางเทคนิคได้

โดย DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า[11] “เนื่องจากระบบการจัดเก็บข้อมูลของธนาคารเกิดขึ้นมาเป็นระยะเวลานานและข้อมูลส่วนบุคคลถูกจัดเก็บข้อมูลส่วนบุคคลในหลากหลายรูปแบบ ทั้งข้อมูลที่อยู่ในระบบและไม่ได้อยู่ในระบบ ทั้งข้อมูลที่สามารถลบได้และข้อมูลที่ไม่สามารถลบได้ จึงก่อให้เกิดปัญหาทางเทคนิคหลายประการ เช่น ไม่สามารถลบข้อมูลส่วนบุคคลตามคำขอของลูกค้าได้เพราะเป็นข้อมูล primary key ที่อยู่ในระบบ หรือไม่สามารถลบได้เพราะเป็นข้อมูลที่ถูกสำรอง (back-up) ไว้นอกระบบ เช่น ถูกบันทึกอยู่ในเทป วัตถุอื่น คอมพิวเตอร์ส่วนตัวของพนักงาน หรือคลาวด์ส่วนตัวของพนักงาน” นอกจากนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่อีก 2 แห่งเห็นว่า “การลงทุนจัดทำข้อมูลนิรนาม (Data Anonymization) ของสถาบันการเงินมีความยุ่งยากเพราะความกระจัดกระจายของข้อมูล และเสียค่าใช้จ่ายเป็นจำนวนมาก”

5.2 บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ผลการสัมภาษณ์พบว่า[12] ปัญหาเกี่ยวกับการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 7 แห่งกล่าวถึง (ขนาดใหญ่ 4 แห่งและขนาดเล็ก 3 แห่ง) ซึ่งสถาบันการเงินขนาดใหญ่ 4 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดเล็ก 2 แห่งให้ความสำคัญเป็นอันดับสอง สถาบันการเงินขนาดเล็กอีก 1 แห่งให้ความสำคัญเป็นอันดับห้า ด้วยเหตุนี้ผู้เขียนจึงจัดให้การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเป็นปัญหาที่มีสำคัญเป็น *‘อันดับสอง’*

[10] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[11] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[12] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity - ROPA) คือ บันทึกที่แสดงรายละเอียดของการดำเนินกิจกรรมในแต่ละครั้ง เช่น ระบุชื่อของผู้ควบคุมข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูล ประเภทของเจ้าของข้อมูล และผู้รับข้อมูลส่วนบุคคลต่อ เป็นต้น โดยหน้าที่การบันทึกบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเบื้องต้นเป็นหน้าที่ของผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูล มิใช่หน้าที่ของ DPO โดยตรง อย่างไรก็ตาม DPO ควรมีส่วนร่วมในการดูแลและให้คำแนะนำในการจัดทำ ROPA ร่วมกับผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลอย่างใกล้ชิด เพื่อทำให้ DPO เข้าใจภาพรวมการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมขององค์กร[13] [14] และตรวจสสอบให้แน่ชัดว่า ROPA ขององค์กรเป็นไปตามกฎหมาย (lawfulness) และมีความเป็นธรรม (fairness)[15]

ส่วนต่อไปนี้ผู้เขียนจะกล่าวถึงปัญหาทางปฏิบัติเกี่ยวกับบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นในสถาบันการเงินผู้ให้สัมภาษณ์ จำนวน 7 แห่ง พร้อมทั้งยกกฎหมายและหลักเกณฑ์อื่นๆ ที่เกี่ยวข้องกับแต่ละประเด็นปัญหาประกอบ โดยแบ่งออกเป็น 2 ประเด็นใหญ่ๆ ได้แก่ (1) ปัญหาภายในสถาบันการเงิน และ (2) การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (LIA)

ภาพที่ 12 ปัญหาทางปฏิบัติในการบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)

- ROPA อาจขาดความถูกต้องและความเป็นปัจจุบัน เนื่องจากกิจกรรมที่เกี่ยวกับข้อมูลส่วนบุคคลของสถาบันการเงินมีจำนวนมหาศาลและเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา ทำให้จำเป็นต้องอาศัยการทำงานแบบบูรณาการกับฝ่ายงานทั้งหมด และขาดเครื่องมือหรือเทคโนโลยีสนับสนุน
- ROPA เป็นงานที่ก่อภาระเพราะใช้พนักงานและเวลาอย่างมาก อีกทั้งปัจจุบันซอฟต์แวร์ในท้องตลาดมีราคาแพง หรืออาจไม่รองรับทุกรายการตามมาตรา 39

[13] Douwe Korff and Marie Georges, "The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation." Ibid. pp.152-155.

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการบันทึกรายการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลและสคส.ตรวจสอบได้ แต่มิให้ห้ามผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ DPO รับผิดชอบหน้าที่ดังกล่าว ทำให้ในทางปฏิบัติ DPO อาจมีหน้าที่จัดทำและเก็บรักษา ROPA โดยอาศัยการรวบรวมข้อมูลจากหลากหลายแผนก/ฝ่ายงานขององค์กรด้วยตัวเอง

[15] Douwe Korff, and Marie Georges. Ibid. pp.172.

- ❖ ความไม่ชัดเจนของกฎหมายโดยเฉพาะอย่างยิ่ง เรื่องการประเมินระหว่างผลประโยชน์โดยชอบธรรมกับสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment - LIA)
- ❖ มีตัวอย่างการกรอกน้อย ผู้ปฏิบัติงาน (โดยเฉพาะอย่างยิ่ง BU) อาจไม่เข้าใจวิธีการกรอกที่เหมาะสม

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

5.2.1 ปัญหาภายในสถาบันการเงิน

กฎหมายกำหนดให้ ROPA ต้องจัดทำเป็นลายลักษณ์อักษรโดยอาจจัดให้อยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอสถาบันการเงินต้องสามารถแสดงให้ สคส. ตรวจสอบได้อย่างรวดเร็ว และต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้[16]

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้มีคำอธิบายประเภทเจ้าของ ข้อมูลส่วนบุคคลและประเภทของข้อมูลส่วนบุคคลด้วย
2. วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลแต่ละประเภท
3. ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ
4. ระยะเวลาในการเก็บรักษาและการลบข้อมูลส่วนบุคคลประเภทต่าง ๆ
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น
6. การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประเภทของผู้ที่อาจได้รับการเปิดเผยข้อมูลและข้อมูลเกี่ยวกับการโอนข้อมูลส่วนบุคคลออกไปยังประเทศที่สามหรือองค์การระหว่างประเทศ (ถ้ามี)
7. คำอธิบายทั่วไปเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (มาตรการเชิงองค์กร และ มาตรการเชิงเทคนิค)

[16] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีบันทึกรายการกิจกรรมประมวลผล ข้อ 2.2. โปรดดู https://www.law.chula.ac.th/event/10941/

ด้วยเหตุนี้ในทางปฏิบัติ เนื่องจากสถาบันการเงินจะการเก็บรวบรวมข้อมูลส่วนบุคคลและมีกิจกรรมการประมวลผลข้อมูลเป็นจำนวนมาก ฉะนั้น การจัดทำ เก็บบันทึก และตรวจสอบ ROPA ตามรายการข้างต้นจึงเกิดภาระอย่างมากแก่องค์กรทั้งในแง่ของจำนวนพนักงานและในแง่ของเวลาที่ใช้ในการดำเนินการ โดยเฉพาะอย่างยิ่งสถาบันการเงินขนาดเล็กจะได้รับผลกระทบดังกล่าวมากกว่าสถาบันการเงินอื่น อีกทั้งกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของฝ่ายงาน/ส่วนงานต่างๆ มีการเปลี่ยนแปลงอย่างรวดเร็ว จึงมีความจำเป็นที่จะต้องใช้กำลังคนเป็นจำนวนมากควบคู่กับระบบค้นหาข้อมูลและบริหารจัดการข้อมูลภายในองค์กรที่เหมาะสม ผู้เขียนจึงคาดว่าสถาบันการเงินแต่ละแห่งซึ่งเป็นผู้ให้สัมภาษณ์อาจพบปัญหาเกี่ยวกับการจัดทำ ROPA ในลักษณะดังกล่าวเช่นเดียวกัน

จากการสัมภาษณ์[17] พบว่า สถาบันการเงินแต่ละแห่งประสบปัญหา ROPA ขาดความถูกต้องและขาดความเป็นปัจจุบัน เนื่องจากข้อมูลส่วนบุคคลมีความกระจัดกระจายของข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลที่ถูกจัดเก็บก่อนช่วงการออกพระราชบัญญัติฯ ทำให้สถาบันการเงินหลายแห่งไม่อาจมั่นใจได้ว่าได้ดำเนินการจัดทำ ROPA อย่างถูกต้องครบถ้วน สถาบันการเงินหลายแห่งยังขาดระบบงานจัดการข้อมูลส่วนบุคคลที่เหมาะสม ดังจะเห็นได้จากการที่ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งให้สัมภาษณ์ว่า “กิจกรรมที่เกี่ยวกับข้อมูลส่วนบุคคลมีจำนวนมหาศาลและเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา จึงจำเป็นต้องอาศัยการทำงานแบบบูรณาการระหว่างแต่ละฝ่ายงานทั้งหมด และมีเครื่องมือที่ใช้ในการอัพเดท ROPA ให้มีความถูกต้องและเป็นปัจจุบันอยู่เสมอ”

อีกประการหนึ่ง การจัดทำ ROPA ของแต่ละสถาบันการเงินเป็นงานที่สร้างภาระแก่องค์กร เพราะใช้พนักงานและเวลาดำเนินการเป็นอย่างมาก ดังที่ DPO ของสถาบันการเงินขนาดเล็กหนึ่งแห่งมีความเห็นว่า[18] “กิจกรรมการประมวลผลขององค์กรในปัจจุบันมีจำนวนไม่ต่ำกว่า 700 รายการ หน้าที่ในการจัดทำ ROPA จึงเป็นงานที่ก่อภาระเป็นอย่างมาก ประกอบกับซอฟต์แวร์ในท้องตลาดปัจจุบันมีราคาแพง” ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งเสริมว่า

[17] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[18] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

“ซอฟต์แวร์ที่วางจำหน่ายในตลาดปัจจุบันนั้นไม่ได้รองรับการบันทึกทุกรายการตามมาตรา 39 องค์กร ในเบื้องต้นจึงต้องใช้ Microsoft Excel แก้ไขปัญหาชั่วคราวแทน”

5.2.2 การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment - LIA)

ประเด็นสำคัญประการหนึ่งที่ DPO ต้องทบทวนและตรวจสอบจาก ROPA ของแต่ละฝ่ายงาน/ส่วนงาน ต่างๆ ภายในสถาบันการเงิน คือ แต่ละฝ่ายงาน/ส่วนงานภายในสถาบันการเงิน[19] ใช้ฐานใดในการประมวลผลข้อมูลส่วนบุคคล (lawful basis) สำหรับแต่ละกิจกรรม (ประเด็นอื่นที่อยู่ในขอบข่ายการตรวจสอบของ DPO นอกจากฐานในการประมวลผลนั้น ผู้เขียนได้กล่าวไว้แล้วใน “หัวข้อ 3.1.2 การทบทวนการประมวลผลให้เป็นไปตามหลักการของกฎหมาย”)

สำหรับการประมวลผลข้อมูลส่วนบุคคลโดยใช้ฐานประโยชน์โดยชอบธรรม (Legitimate Interest) กฎหมายกำหนดให้ สถาบันการเงินสามารถประมวลผลข้อมูลส่วนบุคคลของลูกค้าในกรณีที่จำเป็นต่อการดำเนินการเพื่อประโยชน์โดยชอบธรรมของตนหรือของบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล[20] กล่าวคือ เมื่อผลประโยชน์โดยชอบธรรมอาจไม่สอดคล้องกับประโยชน์ของเจ้าของข้อมูลเสมอไป การประมวลผลข้อมูลส่วนบุคคลของสถาบันการจะต้องชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบของสถาบันการเงินกับสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล (Legitimate Interest Assessment - LIA) โดยอยู่ภายใต้ขอบเขตที่เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้อย่างสมเหตุสมผล (reasonable expectation)[21] เช่น การป้องกัน

[19] ในทางปฏิบัติแต่ละองค์กรควรจัดทำบันทึกรายการกิจกรรมการประมวลผลแยกเป็นรายกิจกรรมตามฝ่ายงาน เพื่อให้ง่ายต่อการดำเนินการ

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5)

[21] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guidlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 90. (สถาบันการเงินไม่อาจอ้างได้ว่าเจ้าของข้อมูลส่วนบุคคลควรจะคาดหมายการประมวลผลข้อมูลได้ เพราะประกาศไว้ในนโยบายความเป็นส่วนตัวไว้แล้ว หากเนื้อหานั้นไม่ได้เฉพาะเจาะจงและสามารถมั่นใจได้ว่าเจ้าของ

อาชญากรรมและการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การรักษาความสัมพันธ์และการจัดการข้อร้องเรียนกับลูกค้า การแจ้งเตือนเพื่อชำระหนี้หรือต่ออายุกองทุนหรือกรมธรรม์ที่สถาบันการเงินเป็นนายหน้า การปฏิบัติตามกฎหมายของต่างประเทศที่จำเป็น เป็นต้น[22]

จะเห็นได้ว่ากฎหมายกำหนดขอบเขตของการใช้ฐานประโยชน์โดยชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลไว้อย่างกว้างและค่อนข้างยืดหยุ่นในการปรับใช้ สถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลจะต้องใช้ดุลพินิจอย่างมากเพื่อระบุ “ประโยชน์โดยชอบธรรมที่จะได้รับ” “ความจำเป็นของการประมวลผลข้อมูลส่วนบุคคล” และ “ชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล” หรือที่เรียกว่า ‘Three Part Test’ ในการนี้สถาบันการเงินอาจร่วมมือกันพัฒนาแนวปฏิบัติที่ใช้เป็นมาตรฐานการให้บริการในแต่ละเรื่องให้เป็นไปในแนวทางเดียวกัน เพื่อให้ลูกค้าสามารถคาดหมายผลประโยชน์ดังกล่าวได้ นอกจากนี้ สถาบันการเงินมีหน้าที่ปกป้องคุ้มครอง “สิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล” ให้สมดุลกับประโยชน์โดยชอบธรรมที่องค์กรจะได้รับ[23]

ข้อมูลส่วนบุคคลจะมีโอกาสได้อ่านจริงๆ เนื่องจากโดยทั่วไปแล้วในยุคปัจจุบัน เราไม่อาจคาดหมายให้ทุกคนอ่านนโยบายความส่วนตัวอย่างละเอียดได้)

[22] ผู้เขียนรวบรวมจาก ICO, "How do we apply legitimate interests in practice?," [Online] Accessed: 2 Nov 2021. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ และ สมาคมธนาคารไทย, แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร สมาคมธนาคารไทย (Guideline on Personal Data Protection for Thai Banks), หน้า.28-34.

[23] การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบขององค์กรกับสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล (LIA) ควรประเมินปัจจัย 3 อย่างได้แก่ 1. ลักษณะของข้อมูล (nature of the data) และบริบทของความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (nature of relationship) 2. ผลกระทบและความเสี่ยงที่จะเกิดขึ้นจากการประมวลผล (potential impact) และ 3. มาตรการปกป้องข้อมูลและคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล (safeguard). เรียบเรียงจาก ICO, "How do we apply legitimate interests in practice?". Ibid.

ตารางที่ 42 การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment – LIA/Three Part Test)

ประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคล	
ขั้นที่ 1 ระบุผลประโยชน์โดยชอบธรรม (Purpose test)	- วัตถุประสงค์ในการประมวลผลคืออะไร? - การประมวลผลนั้นตรงกับวัตถุประสงค์ขององค์กรหรือไม่? - การประมวลผลนั้นเป็นไปเพื่อวัตถุประสงค์ของบุคคลที่สามหรือไม่? - องค์กรได้ปฏิบัติตามกฎหมาย แนวปฏิบัติที่เกี่ยวข้อง หรือจริยธรรมในการประมวลผล (ethic of processing) หรือไม่?
ขั้นที่ 2 ระบุความจำเป็นในการประมวลผล (Necessity test)	- การประมวลผลนั้นสำคัญต่อวัตถุประสงค์ขององค์กรอย่างไร? - การประมวลผลนั้นสำคัญอย่างไรต่อบุคคลที่สามข้อมูลที่ได้รับการเปิดเผย? - มีวิธีอื่นในการบรรลุวัตถุประสงค์เดียวกันนั้นหรือไม่? - สามารถประมวลผลโดยอาศัยฐานอื่นได้หรือไม่?
สิทธิและประโยชน์ของเจ้าของข้อมูล	
ขั้นที่ 3 ชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมขององค์กร กับ ประโยชน์ของเจ้าของข้อมูล (Balancing test)	- เจ้าของข้อมูลคาดหมายได้หรือไม่ว่าการประมวลผลจะเกิดขึ้น? - การประมวลผลสร้างประโยชน์ให้กับผลิตภัณฑ์ หรือบริการที่เจ้าของข้อมูลใช้อยู่หรือไม่? - การประมวลผลส่งผลกระทบในเชิงลบต่อสิทธิของเจ้าของข้อมูลหรือไม่? - การประมวลผลจะส่งผลเป็นอันตรายต่อเจ้าของข้อมูลหรือไม่?
มาตรการคุ้มครองและเยียวยาเจ้าของข้อมูล (Safeguard)	- ข้อมูลส่วนบุคคลถูกเก็บรวบรวมมาอย่างไร? - เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งเกี่ยวกับการประมวลผลข้อมูลหรือไม่? อย่างไร? - องค์กรมีความสัมพันธ์กับเจ้าของข้อมูลอย่างไร? - ที่ผ่านมาองค์กรประมวลผลของเจ้าของข้อมูลเหล่านั้นอย่างไร? - ข้อมูลนั้นเป็นข้อมูลที่มีความอ่อนไหวมากพิเศษ ข้อมูลประวัติอาชญากรรม หรือมีลักษณะที่คนส่วนใหญ่คิดว่ามีความเป็นส่วนตัว (private) สูงหรือไม่ (เช่น ข้อมูลทางการเงิน)? - เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลได้บ้างหรือไม่? - การสร้างสมดุลระหว่างผลประโยชน์อันชอบธรรมขององค์กรกับสิทธิของเจ้าของข้อมูลเกิดขึ้นอย่างไร?

	- การประมวลผลข้อมูลเป็นการรุกล้ำความเป็นส่วนตัวอย่างมากหรือไม่เหมาะสม หรือถูกมองว่าเป็นเช่นนั้นได้หรือไม่? - มีมาตรการอะไรในการป้องกันความเสียหายที่อาจเกิดขึ้นการใช้ข้อมูลนี้หรือไม่?

ที่มา: ผู้เขียนรวบรวมจาก แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines Version 3.0 Extension). หน้า 91-92. และ ICO. How do we apply legitimate interests in practice?

ส่วนในทางปฏิบัติของสถาบันการเงินนั้น จากการสัมภาษณ์พบว่า หน่วยธุรกิจของสถาบันการเงินผู้ให้สัมภาษณ์ส่วนใหญ่ไม่เข้าใจวิธีการกรอก ROPA ดังจะเห็นได้จากการที่ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า[24] “เนื่องจากแบบฟอร์มมาตรฐานของ ROPA ตามกฎหมายยังขาดความชัดเจนและมีตัวอย่างในการกรอกน้อย ประกอบกับปัญหาการตีความเรื่องฐานการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) โดยเฉพาะอย่างยิ่งประเด็นเกี่ยวกับการประเมินระหว่างผลประโยชน์โดยชอบธรรมกับสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (LIA) ทำให้หน่วยธุรกิจขององค์กรเข้าใจการกรอกได้ยาก” เช่นเดียวกับที่เจ้าหน้าที่อาวุโสฝ่ายกฎหมายของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งกล่าวว่า “การทำ ROPA ของสถาบันการเงินอยู่ในระหว่างการทบทวนคุณภาพ เนื่องจากกฎหมายยังมีความใหม่และมีความไม่ชัดเจนสูง ทำให้ผู้ปฏิบัติงานอาจไม่เข้าใจวิธีการกรอกที่เหมาะสม จึงจำเป็นต้องหาเครื่องมือหรือเทคโนโลยีมาช่วยดำเนินการ”

5.3 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล[25]

ผลการสัมภาษณ์พบว่า[26] ปัญหาเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 7 แห่งกล่าวถึง (ขนาดใหญ่ 5

[24] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[25] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ข้อ 2.1. โปรดดู https://www.law.chula.ac.th/event/10941/ “เหตุละเมิดข้อมูลส่วนบุคคล หมายความว่า การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลซึ่งทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง ไม่ว่าจะโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย รวมถึงการเปิดเผย หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน เก็บรวบรวม หรือประมวลผลข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับอนุญาต”

[26] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

แห่ง และขนาดเล็ก 2 แห่ง) ซึ่งสถาบันการเงินขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสาม สถาบันการเงินขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสี่ สถาบันการเงินขนาดใหญ่อีก 1 แห่งให้ความสำคัญเป็นอันดับห้า ด้วยเหตุนี้ผู้เขียนจึงจัดให้การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเป็นปัญหาที่มีสำคัญเป็น *'อันดับสาม'*

สำหรับส่วนต่อไปนี้ ผู้เขียนจะกล่าวถึงปัญหาเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ที่เกิดขึ้นในสถาบันการเงินผู้ให้สัมภาษณ์ จำนวน 7 แห่ง โดยแบ่งออกเป็น 3 ประเด็น ได้แก่ (1) เกณฑ์การพิจารณาความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (2) กรอบระยะเวลาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล และ (3) กระบวนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล พร้อมยกข้อพิจารณาทางกฎหมายและข้อพิจารณาอื่นๆ ที่เกี่ยวข้องในแต่ละประเด็นปัญหา ดังนี้

ภาพที่ 13 ปัญหาทางปฏิบัติเรื่องการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Notification)

- ❖ เกณฑ์การพิจารณาความเสี่ยงฯ (Data Risk Level) ตามกฎหมายยังขาดความชัดเจน
- ❖ สถาบันการเงินอาจไม่สามารถรายงานต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลได้ทันภายใน 72 ชั่วโมง โดยเฉพาะอย่างยิ่งเหตุละเมิดฯ ที่เกิดขึ้นในช่วงสุดสัปดาห์หรือวันหยุดนักขัตฤกษ์
- ❖ ส่วนทางปฏิบัติ ในปัจจุบัน DPO ของสถาบันการเงินยังไม่พบปัญหาเกี่ยวกับการรับมือเหตุละเมิดฯ เนื่องจากกฎหมายยังไม่มีผลบังคับใช้ ทำให้ DPO ยังไม่เคยมีส่วนร่วมจัดการเหตุละเมิดข้อมูลส่วนบุคคลโดยตรง

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

5.3.1 เกณฑ์การพิจารณาความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

ในการประเมินความเสี่ยง[27] ไม่ใช่ทุกองค์กรจะเหมาะกับเกณฑ์การประเมินความเสี่ยงแบบเดียวกัน ดังนั้นจึงควรกำหนดเกณฑ์การประเมินความเสี่ยงตามหลักการ (principle-

[27] Article 29 Data Protection Working Party (WP29), "Statement on the role of a risk-based approach in data protection legal frameworks," [Online] Accessed: 3 Nov 2021. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf. at para 8. (ความเสี่ยงที่จะเกิดผลกระทบต่อ "สิทธิและเสรีภาพของเจ้าของข้อมูล" รวมถึงสิทธิและเสรีภาพดังต่อไปนี้ สิทธิในการไม่ถูกเลือกกปฏิบัติ เสรีภาพในการแสดงความคิดเห็น เสรีภาพทางความคิดความเชื่อและศาสนา และเสรีภาพในการเคลื่อนย้ายถิ่นฐาน)

based) ที่สามารถปรับเปลี่ยนได้ เพื่อให้องค์กรสามารถนำไปปรับใช้ให้เหมาะสมกับบริบทของตน อย่างไรก็ดีเกณฑ์การประเมินความเสี่ยงของกลุ่มธุรกิจเดียวกัน อาจกำหนดให้เป็นไปในทิศทางเดียวกัน แต่มีช่องว่างให้แต่ละองค์กรสามารถนำไปปรับใช้ให้เหมาะสมกับตัวเองได้[28] ในบริบทของการประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลนั้น อาจกล่าวได้โดยสรุปว่า การบริหารความเสี่ยงควรพิจารณาจาก ROPA เป็นพื้นฐาน ประกอบกับบริบทขององค์กร (context establishment)[29] โดยจะต้องคำนึงถึงประเภทข้อมูลส่วนบุคคล จำนวนข้อมูลส่วนบุคคลที่รั่วไหล จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง และการเข้าถึงได้ยังข้อมูลที่มีการรั่วไหล ทั้งนี้ อาจทำการประเมินความเสี่ยงล่วงหน้าได้ เพื่อประโยชน์ในการแจ้งเหตุละเมิดภายในระยะเวลาที่กฎหมายกำหนด[30]

กรณีที่สถาบันการเงินทำการประเมินความเสี่ยงแล้วพบว่าเป็น “ความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล” สถาบันการเงินมีหน้าที่ต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ก่อนหรืออย่างช้าที่สุดในขณะที่มีการประมวลผลข้อมูลส่วนบุคคล รวมถึงการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่แล้ว[31] โดยกรณีที่จึงถือว่าเป็นความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลนั้น อาจรวมถึงกิจกรรมการประมวลผลข้อมูลที่มีลักษณะดังต่อไปนี้ เช่น[32]

[28] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guidlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 536.

[29] ibid. หน้า.534.

[30] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ข้อ 2.14. โปรดดู https://www.law.chula.ac.th/event/10941/

[31] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ข้อ 2.2. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

[32] ผู้เขียนรวบรวมจาก GDPR, Article 35 และ ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ข้อ 2.2. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

- การประมวลผลอันจะส่งผลให้สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลต้องเสื่อมเสียไป หรือทำให้ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้
- การประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ[33] รวมถึงการโปรไฟลิ่ง (profiling)[34] ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
- การประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลประวัติอาชญากรรม โดยพิจารณาจากจำนวนบุคคลที่เกี่ยวข้อง ปริมาณข้อมูลที่เกี่ยวข้อง ความหลากหลายของข้อมูลที่เกี่ยวข้อง ระยะเวลาการประมวลผลข้อมูลที่เกี่ยวข้อง และขนาดพื้นที่ทางภูมิศาสตร์ของการประมวลผลข้อมูลที่เกี่ยวข้อง
- การประมวลผลข้อมูลเพื่อตัดสินใจต่อตัวเจ้าของข้อมูลส่วนบุคคลอันส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล อย่างไรก็ดีการประมวลผลที่ส่งผลน้อยจนถึงไม่มีผลกระทบต่อบุคคล ไม่ถือว่าเข้าข่ายนี้
- กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ เช่น ศูนย์การค้า ถนนและตรอกซอกซอย ตลาด สถานีรถไฟ หรือห้องสมุดสาธารณะ เป็นต้น

[33] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่มีการระบุคำนิยามที่ชัดเจน อย่างไรก็ดี “การประมวลผลข้อมูลด้วยระบบอัตโนมัติ” อาจเทียบเคียงได้กับคำว่า “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ” ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งหมายถึง “โปรแกรมคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติอื่น ที่ใช้เพื่อที่จะทำให้เกิดการกระทำหรือการตอบสนองต่อข้อมูลอิเล็กทรอนิกส์หรือการปฏิบัติการใด ๆ ต่อระบบข้อมูล ไม่ว่าทั้งหมดหรือแต่บางส่วน โดยปราศจากการตรวจสอบหรือการแทรกแซงโดยบุคคลธรรมดาในแต่ละครั้งที่มีการดำเนินการหรือแต่ละครั้งที่ระบบได้สร้างการตอบสนอง”

[34] GDPR, Article 4(4) “โปรไฟลิ่ง” หมายถึง รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินแง่มุมเกี่ยวกับบุคคล โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลธรรมดาในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล ประโยชน์ของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล

ส่วนตามมาตรฐานความมั่นคงปลอดภัยระบบสารสนเทศ[35] แบ่งกำหนดความเสี่ยงและความร้ายแรงของผลกระทบ (impact level) จากการประมวลผลข้อมูลออกเป็น 3 ระดับ ได้แก่ ระดับสูง (high) ระดับกลาง (moderate) และระดับต่ำ (low) ซึ่งบางองค์กรอาจแบ่งระดับไว้มากกว่านี้ตามความเหมาะสมก็ได้

1. ระดับสูง (High) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีความร้ายแรงหรือเป็นหายนะ (severe or catastrophic adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น
    - เกิดผลกระทบร้ายแรงต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมากจนถึงขนาดที่ไม่สามารถทำหน้าที่หรือให้บริการพื้นฐานหนึ่งหรือมากกว่านั้นขององค์กรได้
    - เกิดความเสียหายร้ายแรงต่อสินทรัพย์ขององค์กร
    - เกิดความเสียหายร้ายแรงทางการเงิน
    - เกิดผลกระทบร้ายแรงต่อบุคคล ถึงขนาดที่เกี่ยวกับความเป็นความตายหรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ความเสียหายร้ายแรงทางร่างกาย สังคม หรือทางการเงิน ทำให้ต้องสูญเสียชีวิต สูญเสียความเป็นอยู่อันปกติสุข หรือถูกหน่วงเหนี่ยวกักขัง เป็นต้น
2. ระดับกลาง (Moderate) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีผลกระทบมาก (serious adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น
    - เกิดผลกระทบมากต่อระบบสารสนเทศทำให้ด้อยประสิทธิภาพลงอย่างมีนัยสำคัญ แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กร
    - เกิดความเสียหายมากอย่างมีนัยสำคัญต่อสินทรัพย์ขององค์กร

[35] ผู้เขียนอ้างอิงตาม US Federal Information Processing Standards (FIPS) Publication 1999, "Standards for Security Categorization of Federal Information and Information Systems," [Online] Accessed: 2 Nov 2021. Available from: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

- เกิดความเสียหายทางการเงินมากอย่างมีนัยสำคัญ
- เกิดผลกระทบมากอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงขนาดที่เกี่ยวกับความเป็นความตาย หรือได้รับบาดเจ็บขั้นร้ายแรงถึงชีวิต เช่น ทำให้เกิดความเสียหายทางการเงินเพราะถูกสวมรอยบุคคลหรือถูกปฏิเสธไม่ให้ประโยชน์บางอย่าง ทำให้ต้องอับอายแก่สาธารณะ ทำให้ถูกเลือกปฏิบัติ ทำให้ถูกแบล็คเมล์ เป็นต้น

3. ระดับต่ำ (Low) ได้แก่ กรณีที่ผลกระทบจากการสูญเสียการรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) มีแนวโน้มที่จะมีอยู่อย่างจำกัด (limited adverse effect) ทั้งในระดับบุคคลและระดับองค์กร เช่น
   - เกิดผลกระทบเล็กน้อยต่อระบบสารสนเทศทำให้สังเกตเห็นได้ว่าด้อยประสิทธิภาพลง แต่ยังคงสามารถทำหน้าที่หรือให้บริการพื้นฐานขององค์กรได้
   - เกิดความเสียหายเล็กน้อยต่อสินทรัพย์ขององค์กร
   - เกิดความเสียหายทางการเงินเพียงเล็กน้อย
   - เกิดผลกระทบเล็กน้อยต่อบุคคล เช่น ทำให้ต้องเปลี่ยนเลขหมายโทรศัพท์ เป็นต้น

ส่วนในทางปฏิบัติ จากการสัมภาษณ์พบว่า เจ้าหน้าที่อาวุโสฝ่ายบริหารความเสี่ยงของธนาคารแห่งประเทศไทย กล่าวว่า[36] “กฎหมายยังขาดความชัดเจนเรื่องเกณฑ์ที่ใช้ประเมินความเสี่ยงของข้อมูลส่วนบุคคล (Data Risk Level) ทำให้เกิดปัญหาในการพิจารณาว่ากรณีใดถือว่ามีความเสี่ยงในระดับต่ำ ระดับกลาง หรือระดับสูง ออกมาเป็นรูปธรรม ตัวอย่างเช่น อย่างไรที่ถือว่าเป็นกรณีเจ้าของข้อมูลบาดเจ็บร้ายแรง” เช่นเดียวกับที่ DPO ของสถาบันการเงินแห่งหนึ่ง กล่าวว่า[37] “กฎหมายยังขาดความชัดเจนเรื่องการกำหนดระดับความเสี่ยงของข้อมูล เช่น ข้อมูลของเจ้าของข้อมูลหนึ่งรายรั่วไหลจะถือว่ามีความเสี่ยงและความร้ายแรงของผลกระทบต่อองค์กรสูงเพียงใด

[36] วีระ ประเสริฐนุกูล ผู้ช่วยผู้อำนวยการฝ่ายบริหารความเสี่ยงภาพรวม ธนาคารแห่งประเทศไทย, "สัมภาษณ์ เรื่อง บทบาทหน้าที่และปัญหาที่เกิดขึ้นจากการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล."

[37] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

5.3.2 กรอบระยะเวลาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ สคส. โดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล[38] โดยมีรายละเอียดที่ต้องแจ้ง ได้แก่ ลักษณะของเหตุละเมิด ประเภทของข้อมูลส่วนบุคคลและจำนวนข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่เกี่ยวข้อง รวมถึง ROPA ที่เกี่ยวข้อง (หากสามารถระบุได้) ชื่อและข้อมูลติดต่อ DPO หรือข้อมูลติดต่ออื่นๆ ของผู้ควบคุมข้อมูล ผลที่อาจจะเกิดขึ้นจากเหตุละเมิด มาตรการในการรับมือ และมาตรการในการเยียวยา[39] ทั้งนี้ DPO อาจร้องขอให้ สคส. อนุญาตขยายระยะเวลาการจัดเตรียม และส่งข้อมูลสำหรับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลนั้นได้ เมื่อ สคส. พิจารณาแล้วพบว่ามีเหตุจำเป็นอันสมควร[40]

ในทางปฏิบัตินั้น ผลการสัมภาษณ์พบว่า[41] ผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่ง ล้วนมีข้อกังวลว่า ด้วยเหตุที่กฎหมายยังขาดความชัดเจนดังที่กล่าวข้างต้น สถาบันการเงินอาจไม่สามารถรายงานต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลทันภายใน 72 ชั่วโมง และต้องการให้กฎหมายผ่อนปรนเรื่องดังกล่าว โดยเฉพาะอย่างยิ่งถ้าเหตุละเมิดข้อมูลส่วนบุคคลเกิดขึ้นในช่วงสุดสัปดาห์หรือวันหยุดนักขัตฤกษ์

5.3.3 กระบวนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล

นอกเหนือจากประเด็นข้างต้น ผู้เขียนได้สอบถามผู้ให้สัมภาษณ์ของสถาบันการเงิน 13 แห่ง เกี่ยวกับการมีส่วนเกี่ยวข้องในการจัดการเหตุละเมิดข้อมูลส่วนบุคคลของ DPO ว่า “สถาบัน

---

[38] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

[39] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ข้อ 2.11. โปรดดู https://www.law.chula.ac.th/event/10941/

[40] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ข้อ 2.14. โปรดดู https://www.law.chula.ac.th/event/10941/

[41] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

การเงินต่างๆ มีกระบวนการรับมือเหตุละเมิดข้อมูลส่วนบุคคลอย่างไรบ้าง และ DPO เข้ามามีส่วนเกี่ยวข้องกับกระบวนการดังกล่าวอย่างไร DPO พบปัญหาใดหรือไม่” รวมถึงได้ทำการสัมภาษณ์เจ้าหน้าที่จาก สคส. ว่า “DPO ควรมีส่วนเกี่ยวข้องกับการจัดการเหตุละเมิดข้อมูลส่วนบุคคล ที่อาจเกิดขึ้นในสถาบันการเงินของตนอย่างไร เพื่อแสดงให้เห็นว่าได้ปฏิบัติหน้าที่ตามกฎหมายอย่างเหมาะสมแล้ว”

สำหรับการมีส่วนร่วมของ DPO ต่อกระบวนการรับมือเหตุละเมิดข้อมูลส่วนบุคคล เจ้าหน้าที่จาก สคส. มีความเห็นว่าควรมีแนวทางในการปฏิบัติดังต่อไปนี้[42]

ภาพที่ 14 คำแนะนำเรื่องกระบวนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล

ที่มา: เรียบเรียงจาก “สัมภาษณ์ ดร.สุนทรีย์ ส่งเสริม, นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 29 กรกฎาคม 2564”

1. กำหนดแผนและแนวปฏิบัติเรื่องการจัดการเหตุละเมิดข้อมูลส่วนบุคคลของสถาบันการเงิน เพื่อรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้องตามกฎหมาย เช่น ธปท. สคส. รวมถึง สกมช. (ในกรณีที่เกิดภัยคุกคามทางไซเบอร์)
2. ประเมินเหตุละเมิดข้อมูลส่วนบุคคล ที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลตามมาตรา 37(4) เพื่อพิจารณาว่าสถาบันการเงินในฐานะผู้ควบคุมข้อมูลมีหน้าที่แจ้งเหตุดังกล่าวต่อบุคคลใดหรือหน่วยงานใดบ้าง

[42] ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, "สัมภาษณ์ เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล."

3. ซักซ้อมการจัดการเหตุละเมิดข้อมูลส่วนบุคคล และการเผชิญกับภัยคุกคามทางไซเบอร์ ตลอดจนแลกเปลี่ยนองค์ความรู้ในเรื่องดังกล่าวระหว่างสถาบันการเงิน

ส่วนทางปฏิบัติของแต่ละสถาบันการเงินนั้นมีแนวทางรับมือกับเหตุละเมิดข้อมูลส่วนบุคคลที่มีลักษณะคล้ายคลึงกัน จากผลการสัมภาษณ์พบว่า[43] แต่ละสถาบันการเงินได้จัดตั้งคณะทำงานรับผิดชอบต่อเหตุละเมิดข้อมูลส่วนบุคคลและกำหนดกระบวนการจัดการเหตุดังกล่าว เช่น สถาบันการเงินขนาดเล็กแห่งหนึ่งกำหนดกระบวนการแจ้งเหตุและการเยียวยา โดยมีฝ่ายงานคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล เพื่อนำเสนอต่อคณะกรรมการคุ้มครองข้อมูล (Data Protection Committee) และให้ DPO พิจารณาว่ามีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลมากเพียงใด ส่วนสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งกำหนดให้หัวหน้าฝ่ายงานที่รับผิดชอบทราบพิจารณาเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงด้านปฏิบัติการ (operational risk event) ก่อน หากประเมินแล้วเกินเกณฑ์ที่กำหนดและเข้าข่ายเหตุละเมิดข้อมูลส่วนบุคคลจะต้องส่งเรื่องให้ DPO และคณะทำงานฯ ที่เกี่ยวข้องต่อไป ตลอดจนสถาบันการเงินแต่ละแห่งได้ดำเนินการซักซ้อมระบบรักษาความปลอดภัยของข้อมูล (Data Leakage Protection) ตามที่ ธปท. กำหนดเป็นประจำทุกปี โดยมีแผนจะจัดให้มีตรวจสอบการรั่วไหลข้อมูลส่วนบุคคลเพิ่มเติมลงไป

5.4 การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ผลการสัมภาษณ์พบว่า[44] ปัญหาในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Request - DSR) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 5 แห่งกล่าวถึง (ขนาดใหญ่ 2 แห่ง และขนาดเล็ก 3 แห่ง) ซึ่งสถาบันการเงินขนาดเล็ก 2 แห่ง ให้ความสำคัญเป็นอันดับสอง สถาบันการเงินขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสาม ด้วยเหตุนี้ผู้เขียนจึงจัดให้การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นปัญหาที่มีสำคัญเป็น *‘อันดับสี่’*

[43] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[44] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

สำหรับขั้นตอนสำหรับการปฏิบัติหน้าที่ของสถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลร้องขอสามารถสรุปพอสังเขปได้ดังนี้[45]

ภาพที่ 15 ขั้นตอนการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ

ที่มา: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines Version 3.0 Extension). หน้า 172

ในเบื้องต้น การดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลจะต้องดำเนินการโดยไม่มีค่าใช้จ่าย สถาบันการเงินไม่อาจปฏิเสธไม่ดำเนินการตามคำร้องขอได้ เว้นแต่ คำร้องขอดังกล่าวมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้[46]

---

[45] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guidlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 172.

- คำขอของเจ้าของข้อมูลไม่มีมูลหรือไม่สมเหตุสมผล (unfounded)[47] (สถาบันการเงินในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีภาระในการแสดงให้เห็นโดยกระจ่างถึงลักษณะที่แสดงว่าคำขอดังกล่าวไม่มีมูลหรือไม่สมเหตุสมผล)
- มีลักษณะเป็นคำร้องขอฟุ่มเฟือย (excessive)[48]
- ไม่สามารถยืนยันตัวตนของผู้ยื่นคำร้องขอได้
- เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลอื่นๆ[49]

หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธข้างต้น สถาบันการเงินมีสิทธิปฏิเสธไม่ดำเนินการตามคำร้องขอ หรือเรียกเก็บค่าใช้จ่ายตามสมควร โดยพิจารณาถึงค่าใช้จ่ายในการให้ข้อมูล การสื่อสารหรือการปฏิบัติการตามที่ร้องขอร่วมด้วยโดยละเอียด[50] ซึ่งสถาบันการเงินจะต้องดำเนินการภายในระยะเวลา 30 วันนับแต่วันได้รับคำร้องขอ ทั้งนี้ สามารถขยายระยะเวลาในการดำเนินการได้อีก 60 วัน หากปรากฏว่ามีเหตุจำเป็นที่ทำให้ไม่อาจกระทำได้ภายในระยะเวลาที่กำหนด โดยพิจารณาจาก

---

[46] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ข้อ 2.8. โปรดดู https://www.law.chula.ac.th/event/10941/

[47] ICO, "Manifestly unfounded and excessive requests," [Online] Accessed: 30 Oct 2021. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/ (คำร้องขอที่ไม่สมเหตุสมผล (unfounded) ต้องเป็นคำขอที่สมเหตุสมผลตั้งแต่แรกที่มีการร้องขอ โดยความไม่สมเหตุสมผลอาจเกิดขึ้นในกรณีที่เจ้าของข้อมูลร้องขอให้ลบข้อมูล ซึ่งผู้ควบคุมไม่ได้มีหรือจัดเก็บหรือประมวลผลข้อมูลชุดดังกล่าว)

[48] ibid. (คำขอฟุ่มเฟือย (excessive) เป็นคำขอที่มีลักษณะเป็นการร้องขอซ้ำๆ ในเรื่องเดียวกัน หลายครั้งโดยไม่มีเหตุอันสมควร (legitimate reason) โดยทั่วไปคำร้องเข้าถึงข้อมูลเป็นปริมาณมากที่ก่อให้เกิดภาระงานหนักแก่องค์กรไม่ถือว่าเป็นคำขอฟุ่มเฟือย เจ้าของข้อมูลสามารถขอเพื่อค้นหาข้อมูลที่ตนต้องการได้รับได้)

[49] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guidlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 190. Ibid. (โปรดดู ตารางเหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล)

[50] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ข้อ 2.8. โปรดดู https://www.law.chula.ac.th/event/10941/

ความซับซ้อนและจำนวนคำร้องขอประกอบ แต่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 30 วันนับแต่ได้รับคำร้องขอ พร้อมแสดงเหตุผลของความล่าช้านั้น[51]

ทั้งนี้ สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามกฎหมาย ได้แก่[52] สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล (มาตรา 30) สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (มาตรา 31) สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล (มาตรา 32) สิทธิในการขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ (มาตรา 33) สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (มาตรา 34) และสิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (มาตรา 35)

ในส่วนถัดไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติเกี่ยวกับการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสถาบันการเงินผู้ให้สัมภาษณ์ จำนวน 5 แห่ง ข้างต้น

ภาพที่ 16 ปัญหาทางปฏิบัติเรื่องการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (DSR)

- ❖ เนื่องจากข้อมูลส่วนบุคคลของลูกค้าอาจถูกจัดเก็บในหลายระบบ หลายฝ่ายงานภายในองค์กร ทำให้คำขอบางอย่าง แม้จะเป็นการขอใช้สิทธิเพียงสิทธิเดียว ก็อาจใช้เวลานานในการพิจารณาความถูกต้องของข้อมูลที่มีการร้องขอ และมีค่าใช้จ่ายสูงในการดำเนินการ
- ❖ สถาบันการเงินอาจพิจารณาดำเนินการตามคำขอไม่ทันกำหนดระยะเวลา เพราะขาดระบบที่ใช้เชื่อมโยงกับ ROPA โดยเฉพาะอย่างยิ่งถ้าคำขอใช้สิทธินั้นมีความซับซ้อน (เช่น สถาบันการเงินใช้ข้อมูลเพื่อวัตถุประสงค์ทางการตลาดอย่างไรบ้าง) ไม่อาจพิจารณาจาก ROPA อย่างเดียวได้
- ❖ ขาดแนวปฏิบัติที่เพียงพอสำหรับการดำเนินการ เช่น สถาบันการเงินควรมี protocol message standard, layout portable file หรือ channel ใดบ้าง
- ❖ ความชัดไม่เจนของตัวบทกฎหมายในเรื่องต่างๆ เช่น ขอบเขตการขอใช้สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (มาตรา 31)

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

[51] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ข้อ 2.4. โปรดดู https://www.law.chula.ac.th/event/10941/

[52] GDPR, Article 22 กำหนดให้เจ้าของข้อมูลมีสิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว นอกเหนือจากสิทธิที่ได้กล่าวไว้ข้างต้นด้วย

จากการสัมภาษณ์พบว่า[53] เนื่องจากความไม่ชัดเจนของกฎหมายทำให้เกิดปัญหาในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลหลากหลายด้าน

- DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง แสดงความกังวลว่า “สถาบันการเงินอาจไม่สามารถดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด” โดยเจ้าหน้าที่อีกท่านหนึ่งจากสถาบันการเงินเดียวกัน เสริมว่า “เนื่องจากสถาบันการเงินยังขาดระบบที่ใช้ในการเชื่อมโยงกับ ROPA เช่น Robotic Process Automation - RPA จึงไม่ทราบว่าข้อมูลของลูกค้าถูกจัดเก็บอยู่ในรูปแบบใด อยู่กับฝ่ายงานใดบ้าง หรือใช้ฐานการประมวลผลใด อันจะนำมาใช้ในการพิจารณาสิทธิของลูกค้า โดยเฉพาะอย่างยิ่งในกรณีคำขอใช้สิทธิที่มีความซับซ้อน อันก่อให้เกิดภาระงานที่มากขึ้นเพราะไม่สามารถพิจารณาจากบันทึกฯ แต่เพียงอย่างเดียวได้ เช่น ลูกค้าต้องการทราบว่าธนาคารใช้ข้อมูลส่วนบุคคลทำการตลาดอะไรบ้าง หรือใช้ฐานการประมวลผลข้อมูลส่วนบุคคลอื่นนอกจากฐานความยินยอมหรือไม่”
- DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งกล่าวว่า “การจัดการคำขอใช้สิทธิของสถาบันการเงินเป็นเรื่องที่กระทบต่อความคาดหวังของลูกค้าและสร้างภาระงานเป็นจำนวนมากแก่ผู้ควบคุมข้อมูล สถาบันการเงินแต่ละแห่งจึงต้องการความชัดเจนของกฎหมายลำดับรองในเรื่องต่างๆ เช่น ขอบเขตการใช้สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคลตามมาตรา 31 โดยเรื่องที่ไม่มีกฎหมายหรือแนวปฏิบัติที่มีรายละเอียดเพียงพอสำหรับการดำเนินการ เช่น สถาบันการเงินควรมี layout portable file หรือ channel ใดบ้าง สถาบันการเงินควรจัดทำ protocol message standard อย่างไร”
- DPO ของสถาบันการเงินขนาดเล็กอีกแห่งหนึ่งชี้ให้เห็นว่า เนื่องจากข้อมูลส่วนบุคคลของลูกค้าอาจถูกจัดเก็บไว้ในหลายระบบ หลายฝ่ายงาน อย่างกระจัดกระจาย จึงทำให้ต้องใช้เวลานานในการพิจารณาความถูกต้องของข้อมูล นอกจากนี้ ยังเสริมว่า “การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลรายหนึ่งถึงแม้ว่าจะมีการขอใช้สิทธิตามกฎหมายเพียงสิทธิเดียวก็อาจมีค่าใช้จ่ายจำนวนมากได้”

[53] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

5.5 แบบฟอร์มขอความยินยอม

ผลการสัมภาษณ์พบว่า[54] ปัญหาในการจัดทำแบบฟอร์มขอความยินยอม (Consent Form) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 4 แห่งกล่าวถึง (ขนาดใหญ่ 2 แห่ง และขนาดเล็ก 2 แห่ง) ซึ่งสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดใหญ่ 1 แห่ง และขนาดกลาง 1 แห่งให้ความสำคัญเป็นอันดับสอง สถาบันการเงินขนาดใหญ่อีก 1 แห่งให้ความสำคัญเป็นอันดับเจ็ด ด้วยเหตุนี้ผู้เขียนจึงจัดให้การจัดทำแบบฟอร์มขอความยินยอมเป็นปัญหาที่มีสำคัญเป็น *'อันดับห้า'*

ตามที่ได้กล่าวมาแล้วใน "หัวข้อ 3.1.3 การตรวจสอบประกาศแจ้งการประมวลผลข้อมูล (Privacy Notice) และแบบฟอร์มขอความยินยอม (Consent Form)" แบบฟอร์มขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นเอกสารหลักๆ ที่มีความสำคัญต่อการประมวลผลข้อมูลขององค์กร สถาบันการเงินมีหน้าที่ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมและการประมวลผล เพื่อขอความยินยอมจากเจ้าของข้อมูลในแต่ละกิจกรรม และต้องไม่ทำการเก็บรวบรวมหรือประมวลต่อไปหากเจ้าของข้อมูลถอนความยินยอม ทั้งนี้ วัตถุประสงค์ดังกล่าวต้องเป็นวัตถุประสงค์ที่สมเหตุสมผล

แบบฟอร์มขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลของสถาบันการเงินจะต้องเป็นไปตามหลักเกณฑ์และเงื่อนไขที่หน่วยงานกำกับดูแลกำหนด โดยที่ไม่ขัดต่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ[55] ซึ่งตามประกาศของธนาคารแห่งประเทศไทยนั้นมีการกำหนดหลักเกณฑ์บางประการในการขอความยินยอมจากลูกค้า ในกรณีที่สถาบันการเงินขอความยินยอมเพื่อวัตถุประสงค์ทางการตลาด โดยมีหลักเกณฑ์ ดังนี้[56]

1. ในกรณีที่สถาบันการเงินขอต้องการจะขอความยินยอมในการเปิดเผยข้อมูลของลูกค้าเพื่อวัตถุประสงค์ทางการตลาด การขอความยินยอมต้องมีความชัดเจน ในรูปแบบที่ทำให้มั่นใจได้ว่าลูกค้าเป็นผู้ตัดสินใจให้สิทธิด้วยตนเอง และลูกค้าเข้าใจได้ง่ายว่าไม่ใช่

[54] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[55] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ข้อ 2.2. โปรดดู https://www.law.chula.ac.th/event/10941/

[56] เอกสารแนบ 6 ตาม ประกาศธนาคารแห่งประเทศไทยที่ สกส. 1/2561 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ข้อ 6.2 การเปิดเผยข้อมูลลูกค้าให้แก่บุคคลอื่น

เงื่อนไขการใช้ผลิตภัณฑ์ เช่น แยกส่วนที่ขอความยินยอมเพื่อวัตถุประสงค์ทางการตลาดและเพื่อวัตถุประสงค์อื่นที่ไม่ใช่การตลาดออกจากกัน มีถ้อยคำระบุไว้ที่ด้านบนแบบฟอร์มการขอความยินยอมว่าไม่มีผลต่อการพิจารณาการใช้ผลิตภัณฑ์

2. แบบฟอร์มการขอความยินยอมดังกล่าว ต้องแจ้งวัตถุประสงค์การขอความยินยอมเพื่อการตลาดให้ลูกค้าทราบอย่างชัดเจน เช่น เพื่อการส่งเสริมการขายผลิตภัณฑ์อื่น เพื่อประชาสัมพันธ์เกี่ยวกับบริการต่างๆ เป็นต้น
3. แจ้งรายชื่อผู้รับข้อมูลให้ลูกค้าทราบ เพื่อประกอบการพิจารณาให้ความยินยอม โดยในกรณีที่ผู้รับข้อมูลเป็นบริษัทที่อยู่ในกลุ่มธุรกิจทางการเงิน ผู้ให้บริการสามารถอ้างอิงรายชื่อในแหล่งอื่น เช่น เว็บไซต์ของผู้ให้บริการ โดยอธิบายช่องทางอย่างชัดเจนเพื่อให้ลูกค้าเข้าถึงข้อมูลได้โดยง่าย

   กรณีการเพิ่มรายชื่อผู้รับข้อมูลในภายหลังสำหรับกลุ่มที่ลูกค้าเลือกเปิดเผยข้อมูล ให้แจ้งรายชื่อผู้รับข้อมูลรวมถึงสิทธิและช่องทางในการปฏิเสธการส่งข้อมูล ให้ลูกค้าพิจารณาล่วงหน้า และให้ระยะเวลานานเพียงพอสำหรับลูกค้าในการปฏิเสธการส่งข้อมูล เช่น 30 วัน โดยหากไม่ได้รับการปฏิเสธจากลูกค้าในระยะเวลาที่กำหนด ให้ถือว่าลูกค้ายินยอมให้ส่งข้อมูลให้ผู้รับข้อมูลตามที่ผู้ให้บริการได้แจ้งไป (opt out) ทั้งนี้ต้องมีกระบวนการที่ทำให้มั่นใจว่าลูกค้าได้รับแจ้งข้อมูลข้างต้น
4. แจ้งช่องทางที่ลูกค้าสามารถติดต่อได้อย่างสะดวกเพื่อสอบถามรายชื่อผู้รับข้อมูลและยกเลิกการติดต่อจากผู้รับข้อมูลทุกราย โดยในกรณีที่ลูกค้าเลือกไม่รับการติดต่อจากผู้รับข้อมูล ผู้ให้บริการต้องมีระบบที่สามารถดาเนินการเพื่อไม่ให้มีการติดต่อลูกค้าให้เสร็จสิ้นโดยเร็ว เช่น ภายใน 48 ชั่วโมงหลังจากที่ได้รับแจ้ง ทั้งนี้ หากมีเหตุอันสมควรที่ไม่สามารถดำเนินการได้ทันที ต้องดำเนินการเพื่อไม่ให้มีการติดต่อลูกค้าโดยไม่ชักช้า เช่น ภายใน 10 วัน ทั้งนี้ ต้องดำเนินการให้เสร็จสิ้นโดยเร็ว นับแต่วันที่ได้รับแจ้งจากลูกค้า

นอกเหนือจากหลักเกณฑ์ของแบบฟอร์มขอความยินยอมในกรณีข้างต้น ปัจจุบันยังไม่ปรากฏว่าหน่วยงานกำกับดูแลที่เกี่ยวข้องได้ออกแบบหรือข้อความในการข้อความยินยอมอื่นใด อันมีลักษณะ

เป็นแบบในการขอความยินยอมที่มีสภาพบังคับทางกฎหมาย (compulsory standard form)[57] ประกอบกับยังไม่มีการจัดทำแบบฟอร์มขอความยินยอมสมาคมหรือกลุ่มอุตสาหกรรมที่เกี่ยวข้อง ซึ่งมีลักษณะเป็นแบบหรือข้อความในการขอความยินยอมที่เป็นมาตรฐานแต่ไม่มีสภาพบังคับ (voluntary standard form) (มีวัตถุประสงค์เพื่อจะช่วยให้ปฏิบัติตามกฎหมายได้ง่ายขึ้นในส่วนที่เป็นประเด็นหลัก แม้ไม่ได้มีสภาพบังคับตามกฎหมาย)[58]

โดยส่วนต่อไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติที่เกิดขึ้นจากการจัดทำแบบฟอร์มขอความยินยอมในสถาบันการเงินผู้ให้สัมภาษณ์จำนวน 4 แห่ง ข้างต้น

ภาพที่ 17 ปัญหาทางปฏิบัติเรื่องแบบฟอร์มขอความยินยอม (Consent Form)

- ข้อกังวลว่าแบบฟอร์มของสถาบันการเงินมีความเคร่งครัดมากเกินไป และไม่เป็นมิตรกับลูกค้า
- สถาบันการเงินที่มีธุรกรรม ผลิตภัณฑ์ การให้บริการ เป็นจำนวนมาก ต้องจัดทำแบบฟอร์มขอความยินยอมเฉพาะเรื่อง (specific consent form) ออกมาอย่างไม่มีที่สิ้นสุด

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

สำหรับปัญหาทางปฏิบัติของสถาบันการเงินต่างๆ ในการจัดทำแบบฟอร์มขอความยินยอมนั้น จากการสัมภาษณ์พบว่า[59] ความไม่ชัดเจนของกฎหมายในเรื่องแบบฟอร์มขอความยินยอม จึงอาจทำให้ต้องแต่ละสถาบันการเงินต้องทำการแก้ไขแบบฟอร์มขอความยินยอมใหม่ เมื่อมีกฎหมายลำดับรองออกมาในภายหลัง ดังจะเห็นได้จากการที่ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง[60] กล่าวว่า “การขอความยินยอมจากลูกค้าในการใช้ข้อมูลส่วนบุคคลมีความรัดกุมมากกว่าการขอความยินยอมของสถาบันการเงินแห่งอื่น จึงมีข้อกังวลว่าแบบฟอร์มขององค์กรอาจไม่เป็นมิตรกับลูกค้า และกำลังหาวิธีการแก้ไขให้เกิดความสมดุลเพื่อการปฏิบัติตามกฎหมายและเพื่อประโยชน์ต่อธุรกิจของสถาบันการเงิน”

[57] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ข้อ 2.2. โปรดดู https://www.law.chula.ac.th/event/10941/

[58] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ข้อ 2.3. โปรดดู https://www.law.chula.ac.th/event/10941/

[59] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[60] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

นอกจากนี้ DPO ของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่ง[61] กล่าวว่า “เนื่องจากองค์กรมีธุรกรรม ผลิตภัณฑ์ และบริการเป็นจำนวนมาก แบบฟอร์มมาตรฐานเรื่องการขอความยินยอมจากลูกค้าที่มีอยู่นั้นไม่สามารถใช้ได้ครบทุกเรื่อง ธนาคารจึงต้องมีการจัดทำแบบฟอร์มการขอความยินยอมเฉพาะเรื่อง (specific consent form) มากขึ้น อันเป็นการเพิ่มงบประมาณและภาระงานในการบริหารจัดการความยินยอมอย่างไม่สิ้นสุด”

5.6 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ผลการสัมภาษณ์พบว่า[62] ปัญหาเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross-border Data Transfer) โดยเป็นปัญหาที่สถาบันการเงินขนาดเล็ก 2 แห่งกล่าวถึง ซึ่งสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดเล็กอีก 1 แห่งให้ความสำคัญเป็นอันดับหก ด้วยเหตุนี้ผู้เขียนจึงจัดให้ปัญหาเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศ เป็นปัญหาที่มีสำคัญเป็น *‘อันดับหก’*

ตามกฎหมายเรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศนั้น โดยหลักจะต้องเป็นการโอนข้อมูลส่วนบุคคลไปยังผู้รับนอกประเทศไทยซึ่งมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision)[63] ซึ่งอย่างไรจึงจะถือว่าเป็นประเทศหรือองค์การระหว่างประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล “เพียงพอ” นั้น มีข้อพิจารณาดังต่อไปนี้[64]

[61] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[62] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[63] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 วรรคแรก

[64] GDPR, Article 45 para 2 (a)-(c) และ ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ข้อ 2.2. โปรดดู https://www.law.chula.ac.th/event/10941/

ตารางที่ 43 ข้อพิจารณาประเทศ/องค์การระหว่างประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision)

กฎหมาย	องค์กร	พันธกรณีในระดับนานาชาติ
หลักนิติธรรม การคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานในภาพรวมหรือเฉพาะภาค ซึ่งหมายรวมถึงความมั่นคงของรัฐ กลาโหม ความสงบเรียบร้อยของประเทศ กฎหมายอาญา และการเข้าถึงข้อมูลส่วนบุคคลของรัฐ กฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล มาตรการคุ้มครองความมั่นคงปลอดภัย กฎเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศ ตลอดจนประสิทธิภาพในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลและประสิทธิภาพในการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคลที่ถูกโอนโดยหน่วยงานทางปกครองหรือองค์กรตุลาการ	การมีอยู่ของและประสิทธิภาพการทำงานขององค์กรอิสระในประเทศปลายทางหรือองค์การระหว่างประเทศผู้รับโอน ซึ่งมีอำนาจหน้าที่หรือภารกิจในการบังคับใช้กฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายรวมถึง การมีอำนาจอย่างเพียงพอในการช่วยเหลือและให้คำปรึกษากับเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของตน และการร่วมมือกับคณะกรรมการ	การที่ประเทศปลายทางหรือองค์การระหว่างประเทศผู้รับโอนได้เข้าร่วมหรือมีหน้าที่ต้องปฏิบัติตามซึ่งมีผลบังคับทางกฎหมายตามอนุสัญญาหรือตราสารอื่น ตลอดจนการเข้าร่วมในความร่วมมือระดับภูมิภาคหรือพหุภาคีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ที่มา: ผู้เขียนเรียบเรียงจากร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ข้อ 2.2

โดยในกรณีที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพิจารณาแล้วเห็นว่าประเทศปลายทางหรือองค์การระหว่างประเทศผู้รับข้อมูลส่วนบุคคลนั้น มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ให้ทำการออกประกาศ โดยในการออกประกาศให้คณะกรรมการฯ กำหนดวิธีการทบทวน

มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลอย่างน้อยทุก 4 ปี[65]

ส่วนต่อไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติที่เกิดขึ้นเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของสถาบันการเงินผู้ให้สัมภาษณ์ 2 แห่ง ข้างต้น

ภาพที่ 18 ปัญหาทางปฏิบัติเรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer)

- ความไม่ชัดเจนของคำว่า ‘การโอนข้อมูล (Transfer)’ กับ ‘การส่งผ่านข้อมูล (Transit)[66]’
- ความไม่ชัดเจนของเกณฑ์การพิจารณา และตัวอย่างรายชื่อประเทศปลายทาง/องค์การระหว่างประเทศ ที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision)
- อำนาจเจรจาการทำสัญญาโอนข้อมูลส่วนบุคคลระหว่างสถาบันการเงินกับบริษัทข้ามชาติขนาดใหญ่

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

สำหรับปัญหาเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศ จากการสัมภาษณ์พบว่า[67] DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่ง กล่าวถึง ความไม่ชัดเจนของกฎหมายในเรื่องดังกล่าว ได้แก่ ความไม่ชัดเจนของคำนิยามการโอนข้อมูล (Transfer) และการส่งผ่านข้อมูล (Transit)

อีกประการหนึ่ง คือ ปัญหาความไม่ชัดเจนของเกณฑ์การพิจารณาประเทศ/องค์การระหว่างประเทศปลายทางที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision) ผู้ปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง[68] กล่าวว่า “ทั้ง GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยยังขาดความชัดเจนในเรื่องเกณฑ์การพิจารณามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของผู้รับข้อมูลปลายทางกรณีที่มีการโอนข้อมูลไปยังต่างประเทศ และยังไม่มีประกาศรายชื่อประเทศปลายทางดังกล่าว ปัจจุบันทั่วโลกเหลือ

---

[65] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ข้อ 2.3. โปรดดู https://www.law.chula.ac.th/event/10941/

[66] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ข้อ 2.1. โปรดดู https://www.law.chula.ac.th/event/10941/

[67] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[68] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ประเทศที่ได้รับการยอมรับว่ามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอประมาณ 12 ประเทศเท่านั้น[69] ประเทศสหรัฐอเมริกาและประเทศอังกฤษก็หลุดออกจากรายชื่อเนื่องจากมีคดีเกี่ยวพันกับ Facebook และประเด็น Brexit ตามลำดับ”

นอกจากนี้ ผู้ให้สัมภาษณ์ของสถาบันการเงินแห่งหนึ่ง กล่าวว่า[70] “พบปัญหาการเจรจาทำสัญญาโอนข้อมูลส่วนบุคคลไปต่างประเทศ โดยเฉพาะอย่างยิ่งกับบริษัทข้ามชาติขนาดใหญ่ ต้องพยายามเจรจาและรับรองว่าเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินของตนเป็นไปตามมาตรฐานสากล” อันเป็นปัญหาในลักษณะเดียวกันกับปัญหาที่ผู้เขียนจะกล่าวถึงต่อไปใน “หัวข้อ 5.8 ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล”

5.7 ประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล

ผลการสัมภาษณ์พบว่า[71] ปัญหาเกี่ยวกับประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 2 แห่งกล่าวถึง (ขนาดใหญ่ 1 แห่ง และขนาดเล็ก 1 แห่ง) ซึ่งสถาบันการเงินขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับแรก สถาบันการเงินขนาดใหญ่อีก 1 แห่งให้ความสำคัญเป็นอันดับหก ด้วยเหตุนี้ผู้เขียนจึงจัดให้ปัญหาเกี่ยวกับประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล เป็นปัญหาที่มีสำคัญเป็น *‘อันดับเจ็ด’*

หนึ่งในรายละเอียดที่สำคัญของประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล คือ วัตถุประสงค์ในการประมวลผลข้อมูล เจ้าของข้อมูลต้องสามารถทราบได้ว่าจุดประสงค์ที่แท้จริงของการประมวลผลคืออะไร ฉะนั้น หากในประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคลมีถ้อยคำใน

---

[69] European Commission, "Adequacy decisions," [Online] Accessed: 27 Sep 2021. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (ปัจจุบันประเทศที่ได้รับการยอมรับจากคณะกรรมาธิการยุโรป (European Commission) ว่าเป็นประเทศที่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy decisions) จำนวน 12 ประเทศ ได้แก่ อันดอร์รา อาร์เจนตินา แคนาดา หมู่เกาะแฟโร เกิร์นซีย์ อิสราเอล ไอล์ออฟแมน ญี่ปุ่น เจอร์ซีย์ นิวซีแลนด์ สวิตเซอร์แลนด์ และอุรุกวัย)

[70] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[71] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

ลักษณะของการแจ้งวัตถุประสงค์เผื่อไว้อย่างกว้างๆ หรือเป็นการทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ อาจขัดต่อหลักความชัดเจนของการจัดเก็บข้อมูลส่วนบุคคล (Explicit) ได้[72]

ภายหลังจากการได้ข้อมูลส่วนบุคคล โดยหลักนั้นสถาบันการเงินจะต้องใช้หรือเปิดเผยข้อมูลนั้นตามวัตถุประสงค์ที่ผู้ได้แจ้งต่อเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะที่เก็บรวบรวมข้อมูล[73] ไม่สามารถเพิ่มวัตถุประสงค์เองได้ในภายหลัง หากภายหลังสถาบันการเงินต้องการจะใช้ข้อมูลดังกล่าวเพื่อวัตถุประสงค์อื่นๆ ที่ไม่อาจคาดหมายได้ในขณะทำการเก็บรวบรวมข้อมูล[74]

ในส่วนถัดไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติที่เกิดขึ้นเกี่ยวกับประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินผู้ให้สัมภาษณ์ 2 แห่ง ข้างต้น

ภาพที่ 19 ปัญหาทางปฏิบัติเรื่องประกาศแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice)

- ❖ BU ของสถาบันการเงินอาจนำข้อมูลส่วนบุคคลไปใช้เกินขอบเขตวัตถุประสงค์ที่ระบุไว้
- ❖ สถาบันการเงินบางแห่ง (โดยเฉพาะอย่างยิ่งขนาดเล็ก) ไม่มั่นใจในมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในประกาศว่ามีความเพียงพอจริง
- ❖ การแจ้งรายละเอียดการประมวลผลข้อมูลตามมาตรา 23 ให้ครบถ้วนแก่ลูกค้าที่โทรศัพท์มาขอความช่วยเหลือ (เช่น บัตรเครดิตหาย เปิดบัญชีไม่ได้) ใช้เวลานานเกินไปจนอาจทำให้เสียฐานลูกค้าได้

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

[72] GDPR, Article 5(1)(b) กำหนดว่าการจัดเก็บข้อมูลมีไว้เพื่อวัตถุประสงค์ที่เฉพาะเจาะจง (specified) ชัดแจ้ง (explicit) และชอบด้วยกฎหมาย (legitimate) และไม่ถูกประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว (not further processed in a way incompatible with those purposes)

[73] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21 วรรคแรก

[74] Bart Custers and Helena U Vrabec, "Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection," [Online] Accessed: 1 Nov 2021. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046774 (ตัวอย่างเช่น ในทางวิชาการนั้น การนำข้อมูลกลับมาใช้ใหม่ (Data Recycling) เป็นการนำข้อมูลมาใช้เพื่อวัตถุประสงค์แบบเดิมมากกว่า 1 ครั้ง จึงไม่น่าจะเป็นประเด็นในเรื่องของสิทธิในการประมวลผลข้อมูลมากนัก กับการเปลี่ยนแปลงบริบทของข้อมูล (Data Recontextualization) ซึ่งอาจเกิดขึ้นเมื่อมีการโอนขายข้อมูลไปยังผู้ควบคุมข้อมูลอื่น กรณีดังกล่าวก็ไม่มีประเด็นทางกฎหมายเรื่องการแปลงวัตถุประสงค์ใหม่เช่นกัน แต่ในกรณีของการแปลงวัตถุประสงค์ (Repurpose) ผู้ควบคุมข้อมูลจะต้องแจ้งวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลเสมอเว้นแต่จะมีข้อยกเว้นตามกฎหมาย)

จากการสัมภาษณ์พบว่า[75] เจ้าหน้าที่ฝ่ายกำกับการปฏิบัติตามกฎเกณฑ์ของสถาบันการเงินขนาดใหญ่แห่งหนึ่ง กล่าวว่า “ประสบปัญหาที่หน่วยธุรกิจขององค์กรอาจนำข้อมูลส่วนบุคคลไปใช้เกินขอบเขตที่ระบุไว้ในประกาศแจ้งการประมวลผลของสถาบันการเงิน ถึงจะมีการติดต่อประสานงานระหว่าง DPO กับหน่วยธุรกิจเป็นประจำก็ตาม”

ผู้เขียนเห็นว่าหากสถาบันการเงินพบว่ามีความจำเป็นต้องประมวลผลด้วยวัตถุประสงค์ที่แตกต่างจากเดิมที่ได้รับความยินยอมไว้และไม่มั่นใจว่าวัตถุประสงค์ดังกล่าวเป็นวัตถุประสงค์ที่คาดหมายได้ขณะเก็บรวบรวมข้อมูลหรือไม่ ควรขอคำปรึกษาจาก DPO หรือฝ่ายกฎหมายของสถาบันการเงิน ถ้าเป็นการประมวลผลข้อมูลส่วนบุคคลด้วยวัตถุประสงค์ใหม่จริง จะต้องแจ้งวัตถุประสงค์ใหม่และได้รับความยินยอมของเจ้าของข้อมูลส่วนบุคคลก่อนนำข้อมูลนั้นไปประมวลผลตามมาตรา 21(1) และ (2)[76] โดยการแจ้งวัตถุประสงค์ใหม่นี้ ควรมีการอธิบายความจำเป็น ความแตกต่าง รวมถึงผลกระทบที่อาจเกิดขึ้นจากความเปลี่ยนแปลงดังกล่าวให้แก่เจ้าของข้อมูลทราบ ทั้งนี้เพื่อให้เกิดความโปร่งใสและความน่าเชื่อถือแก่ภาพลักษณ์ขององค์กร

ปัญหาเกี่ยวกับประกาศแจ้งการประมวลผลข้อมูลอีกประการหนึ่ง DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่ง[77] กล่าวว่า “เมื่อเจ้าของข้อมูลโทรศัพท์มาขอความช่วยเหลือ เช่น บัตรเครดิตหาย หรือข้อมูลที่มีอยู่ไม่สามารถเบิกบัญชีได้ ฯลฯ สถาบันการเงินมีหน้าที่บันทึกเสียงโทรศัพท์ของลูกค้า แต่ในทางปฏิบัตินั้นการแจ้งรายละเอียดเกี่ยวกับการจัดเก็บและใช้ข้อมูลส่วนบุคคลให้ครบถ้วนตามมาตรา 23 อาจใช้เวลาสอบถามข้อมูลนานเกินไปจนทำให้สูญเสียฐานลูกค้าได้ และเห็นว่าควรมีกฎหมายกำหนดข้อยกเว้นหรือข้อผ่อนปรนในกรณีนี้”

นอกจากปัญหาข้างต้นแล้ว จากการสัมภาษณ์ยังพบว่า DPO ของสถาบันการเงินขนาดเล็กแห่งหนึ่งมีข้อกังวลว่าอาจไม่สามารถปฏิบัติตามกฎหมายเรื่องดังกล่าวได้อย่างครบถ้วน เพราะ

[75] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[76] ถ้าสถาบันการเงินไม่แจ้งวัตถุประสงค์ แล้วทำการประมวลผลข้อมูลส่วนบุคคลโดยไม่ตรงตามวัตถุประสงค์ที่ได้แจ้งไว้ก่อนหรือขณะเก็บรวบรวม ต้องระวางโทษปรับทางปกครองไม่เกิน 3,000,000 บาทตามมาตรา 83 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[77] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

กฎหมายที่มีความไม่ชัดเจนสูง โดยกล่าวว่า[78] “...วิธีการป้องกันที่ดีที่สุดที่ทางองค์กรสามารถทำ ณ ปัจจุบัน คือการนำเทคโนโลยีเข้ามาช่วยในด้านต่างๆ เช่น การป้องกันการรั่วไหลของข้อมูลส่วนบุคคล การจำกัดสิทธิในการเข้าถึงข้อมูล” ที่สะท้อนให้เห็นว่าความไม่ชัดเจนของกฎหมายเรื่อง “มาตรฐานการด้านคุ้มครองข้อมูลส่วนบุคคลขั้นต่ำขององค์กร” นั้นส่งผลกระทบโดยตรงต่อการลงทุนพัฒนาระบบบริหารจัดการข้อมูลของสถาบันการเงินต่างๆ โดยเฉพาะอย่างยิ่งกับสถาบันการเงินขนาดเล็กที่มีงบประมาณและทรัพยากรอย่างจำกัด

5.8 ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

ผลการสัมภาษณ์พบว่า[79] ปัญหาเกี่ยวกับการทำข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ระหว่างผู้ควบคุมและผู้ประมวลผล (Data Processing Agreement) โดยเป็นปัญหาที่สถาบันการเงินจำนวน 3 แห่งกล่าวถึง (ขนาดใหญ่ 2 แห่ง และขนาดเล็ก 1 แห่ง) ซึ่งสถาบันการเงินขนาดใหญ่ 1 แห่งและขนาดเล็ก 1 แห่งให้ความสำคัญเป็นอันดับสี่ สถาบันการเงินขนาดใหญ่อีก 1 แห่งให้ความสำคัญเป็นอันดับห้า ด้วยเหตุนี้ผู้เขียนจึงจัดให้การทำข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เป็นปัญหาที่มีสำคัญเป็น *‘อันดับแปด’* จากปัญหาทั้งหมดที่กล่าวมาแล้วข้างต้น

โดยหลักสัญญาประมวลผลข้อมูลส่วนบุคคลต้องมีองค์ประกอบที่สำคัญ คือ[80] หัวข้อและระยะเวลาของการประมวลผล ลักษณะและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคลและประเภทของเจ้าของข้อมูล และหน้าที่และสิทธิของผู้ควบคุมข้อมูลส่วนบุคคล นอกจากนี้ มักจะมีประเด็นในสัญญาประมวลผลข้อมูลที่สถาบันการเงินและผู้ให้บริการจะต้องเจรจาต่อรองกัน 3 ประเด็นหลัก[81] คือ (1) หน้าที่ในการประมวลผลข้อมูล (Obligation) (2) ความรับผิด (Liability) และ (3) การรับประกัน (Warranty)

---

[78] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[79] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

[80] GDPR, Article 28(3)

[81] ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, Thailand Data Protection Guildlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension), หน้า. 504

สถาบันการเงินสามารถทำสัญญาระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล ในฐานะเป็นสัญญาอุปกรณ์ของสัญญาหลัก กล่าวคือ ทำสัญญาการประมวลผลข้อมูลส่วนบุคคลแยกต่างหากอีกฉบับหนึ่งจากสัญญาฉบับเดิม ซึ่งเป็นสัญญาการขายผลิตภัณฑ์/การให้บริการ หรืออาจเลือกที่จะเพิ่มเติมข้อสัญญาดังกล่าวลงไปในสัญญาฉบับเดิม ซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลนั้นอาจเป็นบริษัทในประเทศไทย หรือบริษัทต่างชาติก็ได้ อย่างไรก็ดี เนื่องจากสภาพกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยยังอยู่ระหว่างการพัฒนาออกกฎหมายลำดับรองกำหนดรายละเอียดในเรื่องต่างๆ จึงอาจทำให้ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นชาวต่างชาติที่ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับสถาบันการเงินไทย มองว่ากฎหมายไทยและกระบวนการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินไทยยังไม่ได้มาตรฐานสากล จึงมีแนวโน้มที่จะกำหนดให้ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

ถัดไปผู้เขียนจะกล่าวถึงปัญหาในทางปฏิบัติที่เกิดขึ้นจากการทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างสถาบันการเงินผู้ให้สัมภาษณ์ จำนวน 3 แห่ง กับคู่ค้า/ผู้ให้บริการภายนอก

ภาพที่ 20 ปัญหาทางปฏิบัติเรื่องข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (DPA)

- ❖ สถาบันการเงินอยู่ในสถานะที่มีอำนาจต่อรองการทำข้อตกลงฯ ต่ำกว่า Data Processor/Vendor โดยเฉพาะยิ่งคู่กรณีที่เป็นชาวต่างชาติ (เช่น มักอ้างว่าเนื้อหาสัญญาที่ตนร่างเป็นไปตาม GDPR ฯลฯ)
- ❖ หากเจรจาตกลงกันไม่ได้ สถาบันการเงินจะต้องเปลี่ยนวิธีการจัดเก็บข้อมูลทำให้เสียค่าใช้จ่ายมาก

ที่มา: บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง

จากการสัมภาษณ์พบว่า[82] ในทางปฏิบัติของสถาบันการเงินเกิดปัญหาเกี่ยวกับอำนาจต่อรองการทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ระหว่างสถาบันการเงินไทยกับผู้ประมวลผลข้อมูลซึ่งเป็นบุคคลภายนอก โดยเฉพาะอย่างยิ่งกรณีบริษัทต่างชาติ ดังที่จะเห็นได้จากการที่ DPO ของสถาบันการเงินขนาดใหญ่แห่งหนึ่งกล่าวว่า “...เช่น บริษัทอเมริกา มักอ้างว่าเนื้อหาของสัญญาการประมวลผลข้อมูลส่วนบุคคลของตนเป็นไปตาม GDPR ทำให้บุคคลที่เกี่ยวต้องพยายามเจรจารับรองว่าเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขององค์กรนั้นเป็นไปตามมาตรฐานสากล” ซึ่ง DPO ของสถาบันการเงินขนาดใหญ่อีกแห่งหนึ่งเสริมว่า “หากคู่ค้าหรือผู้ให้บริการประมวลผลข้อมูลไม่ตกลงทำ

[82] บทสัมภาษณ์, กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง, เรื่องเดิม

สัญญาฯ องค์กรจะต้องเปลี่ยนจากการจัดเก็บข้อมูลในระบบคลาวด์ (Cloud) มาเป็นวิธีอื่น ซึ่งจะเสียค่าใช้จ่ายจำนวนมาก”

ในประเด็นนี้ ผู้เขียนมีความเห็นว่าปัญหาการทำข้อตกลงดังกล่าว เป็นปัญหาที่พบได้บ่อยในสถาบันการเงินขนาดกลางและขนาดเล็กเป็นส่วนใหญ่ และมีแนวโน้มที่จะลดลงมากเมื่อกฎหมายลำดับรองต่างๆ มีความชัดเจนมากขึ้น โดยเฉพาะอย่างยิ่งเรื่อง “มาตรการคุ้มครองที่เหมาะสมสำหรับการประมวลผลข้อมูลส่วนบุคคล” เมื่อเป็นเช่นนั้น สัญญาการประมวลผลข้อมูลส่วนบุคคลที่ทำขึ้นในประเทศไทย ก็ควรกำหนดให้ใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย และควรกำหนดให้เป็นสิทธิโดยเด็ดขาดของสถาบันการเงินซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล

บทที่ 6

บทสรุปและข้อเสนอแนะ

ในอดีตสถาบันการเงินจะทำการเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าและพนักงานไว้เป็นความลับและจะไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลหากไม่ได้รับความยินยอมโดยชัดแจ้ง แต่เนื่องจากข้อมูลส่วนบุคคลกลายเป็นสิ่งที่สามารถนำมาใช้ให้เกิดประโยชน์ได้และเป็นสิ่งที่มีมูลค่าอย่างมากในปัจจุบัน จึงมีความจำเป็นที่สถาบันการเงินซึ่งเป็นหน่วยงานที่ประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากจะต้องหันมาให้ความสำคัญในการแต่งตั้ง DPO ที่มีความรู้ความสามารถเหมาะสม กำหนดโครงสร้างการดำเนินงาน กระบวนการประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลที่ดีแก่องค์กร และสร้างความไว้วางใจแก่เจ้าของข้อมูลส่วนบุคคล

ผู้เขียนทำการศึกษาและวิเคราะห์ปัญหาอันจากบทบัญญัติทางกฎหมายและปัญหาที่เกิดขึ้นจริงในทางปฏิบัติจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล พบว่าสอดคล้องกับสมมติฐานที่ว่า “ในปัจจุบันยังไม่มีการกำหนดโครงสร้างการทำงานและคุณสมบัติของ DPO ในสถาบันการเงินที่ชัดเจน จึงทำให้มีปัญหาการขัดกันของการปฏิบัติหน้าที่ระหว่างบทบาทหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และบทบาทหน้าที่ที่ DPO มีต่อองค์กร รวมถึงปัญหาด้านความสามารถของ DPO”

6.1 บทสรุป

จากการสำรวจพบว่า ปัจจุบันสถาบันการเงินไทย 13 แห่งเลือกที่จะแต่งตั้ง DPO จากบุคคลภายในองค์กร ซึ่งส่วนใหญ่จะเป็นผู้บริหารระดับสูงของฝ่ายงาน/สายงาน เช่น ฝ่ายงานกำกับดูแลการปฏิบัติตามกฎเกณฑ์ ฝ่ายงานกฎหมาย ฝ่ายงาน เทคโนโลยีสารสนเทศ เป็นต้น และมีการรายงานโดยตรงต่อผู้บริหารสูงสุดขององค์กรซึ่งการรายงานดังกล่าวยังไม่มีอุปสรรคหรือสถานการณ์ใดที่ทำให้ DPO ไม่สามารถรายงานไปยังบุคคลดังกล่าวได้ อันเป็นลักษณะเฉพาะที่ทำให้ DPO สถาบันการเงินนั้นมีความแตกต่างจาก DPO ขององค์กรอื่นๆ ที่อาจไม่มีโครงสร้างการรายงานที่มีประสิทธิภาพ ทำให้ไม่สามารถรายงานไปยังผู้บริหารระดับสูงหรือคณะกรรมการภายในองค์กรที่ทำหน้าที่กำกับดูแล

หรือตรวจสอบโดยตรงได้ตามมาตรา 42 วรรคสาม นอกจากนี้ยังพบว่า ลักษณะการปฏิบัติงานของสถาบันการเงินมีส่วนเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลที่เป็นชาวต่างชาติมากกว่าองค์กรธุรกิจอื่น รวมไปถึงกระบวนการบริหารความเสี่ยงของสถาบันการเงินมีหลากหลายด้าน จึงทำให้บุคคลที่ดำรงตำแหน่ง DPO ของสถาบันการเงินเป็นผู้ที่มีความรู้ความเข้าใจแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศและการบริหารจัดการความเสี่ยงในระดับที่สูงกว่า DPO ของภาคธุรกิจอื่น

ในส่วนปัญหาเกี่ยวกับมาตรฐานการปฏิบัติตำแหน่งหน้าที่ DPO ในสถาบันการเงิน พบว่ายังขาดหลักการที่สำคัญที่เกี่ยวข้องกับการปฏิบัติหน้าที่ตำแหน่ง DPO ดังต่อไปนี้

(1) สถาบันการเงินส่วนใหญ่ไม่มีกระบวนการปรึกษาหารือระหว่างฝ่ายงานผู้ใช้ข้อมูลกับ DPO ที่ครอบคลุมวงจรชีวิตของข้อมูล[1] โดยกระบวนการที่มีอยู่นั้นมีลักษณะเป็นการแบ่งประเภทตามประเด็นที่ต้องการปรึกษา หรือแบ่งตามช่องทางการขอคำปรึกษา หรือเป็นเพียงแต่การกำหนดหลักการอย่างกว้างว่าให้มีการปรึกษาหารือกับ DPO ทุกครั้งที่มีผลิตภัณฑ์หรือการบริการใหม่ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล รวมทั้งไม่มีการจัดทำคู่มือและแบบฟอร์มการปรึกษาหารือที่ใช้ในการกำหนดรายละเอียดการถามตอบ ซึ่งอาจทำให้คำตอบในเรื่องเดียวกันไม่เป็นไปในทิศทางเดียวกัน

(2) ขาดพนักงานที่มีความรู้ความเข้าใจและเครื่องมือที่ใช้ในการรักษาความปลอดภัยของข้อมูล[2] แม้คณะกรรมการผู้บริหารของสถาบันการเงินจะให้ความสำคัญถึงการปฏิบัติตามกฎหมาย แต่เนื่องจากพนักงานที่อยู่ในคณะทำงานด้านข้อมูลส่วนบุคคลของสถาบันการเงินแต่ละแห่งมีภาระด้านงานอื่นต่อองค์กรโดยเฉพาะอย่างยิ่งในสถานการณ์ Covid-19 ปัจจุบัน ทำให้พนักงานไม่สามารถใช้เวลากับการทำงานและการหาความรู้เกี่ยวกับการปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคลได้อย่างเต็มที่ ประกอบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องใหม่สำหรับผู้ปฏิบัติงานในสถาบันการเงินไทย ส่งผลให้เกิดความไม่แน่ใจว่าสถาบันการเงินจะต้องลงทุนพัฒนาระบบบริหารจัดการข้อมูลมากน้อยเพียงใดเพื่อให้เป็นไปตามมาตรฐานขั้นต่ำของกฎหมาย

---

[1] รายละเอียดเพิ่มเติมโปรดดู บทที่ 3 หัวข้อ 3.1.1 กระบวนการปรึกษาหารือกับฝ่ายที่ประสงค์จะใช้ข้อมูลในส่วน (1) การกำหนดกระบวนการภายในองค์กร (2) ประเด็นการให้คำปรึกษาและแสดงความเห็น และ (3) บันทึกการให้คำปรึกษาหารือ, หน้า 40-49.

[2] รายละเอียดเพิ่มเติมโปรดดู บทที่ 3 หัวข้อ 3.2 ทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย ในส่วน 3.2.1 บุคลากร และ 3.2.2 เครื่องมือและเทคโนโลยี, หน้า 77-80.

(3) ไม่มีโครงสร้างความเป็นอิสระในการตัดสินใจของ DPO ทำให้ไม่สามารถแบ่งแยกบทบาทหน้าที่ระหว่างบทบาทหน้าที่พนักงานองค์กรกับบทบาทหน้าที่ของ DPO ตามกฎหมาย[3] แม้ DPO ของสถาบันการเงินส่วนใหญ่จะให้สัมภาษณ์ว่าตนมีความเป็นอิสระในการทำงาน สามารถรายงานต่อผู้บริหารสูงสุดขององค์กรได้หากมีความจำเป็น แต่ในทางปฏิบัติไม่ได้มีการกำหนดสายการรายงานตรงต่อผู้ที่มีอำนาจตัดสินใจสูงสุดหรือต่อคณะกรรมการอิสระของสถาบันการเงินอย่างชัดเจน ไม่มีการกำหนดมาตรฐานการรายงานในเรื่องต่างๆ เช่น ประเด็นการคุ้มครองข้อมูลส่วนบุคคลที่ต้องรายงาน บุคคลที่ต้องรายงาน ความถี่ของการรายงาน เป็นต้น อีกทั้งไม่มีหลักการคุ้มครองความเป็นอิสระของ DPO ในสถาบันการเงิน เช่น กระบวนการสอบข้อเท็จจริงในกรณีที่ DPO ถูกผู้บริหารองค์กรลงโทษหรือกระบวนการจากหน่วยงานกำกับดูแลเช่นที่ธนาคารแห่งประเทศไทยดำเนินการเช่นเดียวกับผู้ปฏิบัติหน้าที่ในฐานะ 2nd Line ทั่วไป

(4) สถานะทางกฎหมายของตำแหน่งผู้ช่วย DPO ยังไม่มีการรับรองไว้[4] จากการสำรวจพบว่ามีการแต่งตั้งผู้ช่วย DPO ในสถาบันการไทยทั้ง 13 แห่งซึ่งมีส่วนสำคัญที่จะทำให้งานคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินสัมฤทธิ์ผล และยังเป็นประโยชน์ต่อการกำหนดผู้ที่จะดำรงตำแหน่ง DPO ขององค์กรในอนาคต อย่างไรก็ดี พบว่าสถาบันการเงินแต่ละแห่งไม่ได้ให้ความสำคัญกับการรับรองสถานะความเป็นอิสระและปราศจากความขัดแย้งทางผลประโยชน์ของผู้ช่วย DPO แต่อย่างใด

(5) ไม่มีการกำหนดความรู้ความสามารถหรือคุณสมบัติของ DPO สถาบันการเงินเป็นการเฉพาะ[5] สำหรับความคืบหน้าปัจจุบันตามร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็เป็นการกำหนดคุณสมบัติ DPO เป็นการทั่วไป ยังไม่มีการประกาศคุณสมบัติ DPO สำหรับภาคสถาบันการเงินเป็นการเฉพาะเจาะจง นอกจากนี้ ผู้ให้สัมภาษณ์ส่วนใหญ่เห็นว่าหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลสำหรับ DPO ที่มีอยู่ในประเทศไทยขณะนี้เป็นเพียงหลักสูตรพื้นฐานซึ่งไม่เพียงพอต่อการปฏิบัติงานจริงในองค์กร

[3] รายละเอียดเพิ่มเติมโปรดดู บทที่ 3 หัวข้อ 3.3 ความเป็นอิสระ และหัวข้อ 3.5 ระยะเวลาและการพ้นจากตำแหน่งของ DPO, หน้า 87-94 และหน้า 106-117 ตามลำดับ.

[4] รายละเอียดเพิ่มเติมโปรดดู บทที่ 3 หัวข้อ 3.6 ผู้ช่วย DPO และผู้แทน DPO, หน้า 117-120.

[5] รายละเอียดเพิ่มเติมโปรดดู บทที่ 4 หัวข้อ 4.2 ความรู้ความเข้าใจ และหัวข้อ 4.5 การจัดฝึกอบรมความรู้ภายในสถาบันการเงิน, หน้า 128-140 และหน้า 147-148 ตามลำดับ.

(6) ไม่มีมาตรฐานการทบทวนงานประมวลผลข้อมูลส่วนบุคคลขององค์กรที่ชัดเจน[6] โดยร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดรายการขั้นต่ำในการพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลขององค์กรใดองค์กรหนึ่งเป็นไปตามกฎหมายหรือไม่ จากการสัมภาษณ์พบว่า DPO และผู้ปฏิบัติงานในคณะทำงานด้านข้อมูลส่วนบุคคลของสถาบันการเงินต่างๆ ประสบปัญหาในการตรวจสอบและดำเนินการให้เป็นไปตามกฎหมายหลากหลายประการ เช่น การชั่งน้ำหนักระหว่างผลประโยชน์โดยชอบธรรมกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment - LIA) ระดับความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Data Risk Level) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ ความแตกต่างระหว่างการโอนข้อมูล (Transfer) กับการส่งผ่านข้อมูล (Transit) หรืออำนาจเจรจาต่อรองในการทำข้อตกลงการประมวลผลกับบริษัทต่างชาติ เป็นต้น

โดยมีปัญหาหรืออุปสรรคสำคัญของ DPO ที่สถาบันการเงินต่างๆ และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ต้องให้ความสำคัญอย่างเร่งด่วน ได้แก่

6.1.1 ปัญหาความเป็นอิสระและความขัดแย้งทางผลประโยชน์ของ DPO

ความเป็นอิสระและการปราศจากความขัดแย้งทางผลประโยชน์ของบุคคลที่ดำรงตำแหน่งเป็น DPO ของสถาบันการเงิน เป็นประเด็นปัญหาประการหนึ่งที่สำคัญ โดยสถาบันการเงินต้องมีการกำหนดโครงสร้างการทำงานของ DPO ให้มีความเป็นอิสระ สอดคล้องตามวัตถุประสงค์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เกิดความโปร่งใสของการประมวลผลข้อมูลส่วนบุคคล จึงจำเป็นต้องมีการออกบทบัญญัติหรือแนวปฏิบัติกลางเกี่ยวกับโครงสร้างและมาตรฐานการรายงานของ DPO ที่ชัดเจน โดยเฉพาะอย่างยิ่งเรื่อง ประเด็นด้านข้อมูลส่วนบุคคลที่ต้องรายงาน บุคคลที่จำเป็นต้องรายงาน และความถี่ของการรายงาน

[6] รายละเอียดภาพรวมเกี่ยวกับปัญหาทางปฏิบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินปรากฏอยู่ในตอนต้นของบทที่ 5 โดยลักษณะของปัญหาแต่ละประการ โปรดดูตั้งแต่หัวข้อ 5.1 การเก็บรักษาและการลบข้อมูลส่วนบุคคล ไปจนถึง หัวข้อ 5.8 ข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล, หน้า 154-194.

นอกจากนี้ หน่วยงานกำกับดูแลควรให้ความสำคัญกับการคุ้มครองตำแหน่ง DPO ให้เกิดความเป็นอิสระและปราศจากความขัดแย้งทางผลประโยชน์เช่นเดียวกับที่ธนาคารแห่งประเทศไทยดำเนินการกับผู้ปฏิบัติงานในฐานะ 2nd Line of Defense ทั่วไป โดยจากการสำรวจพบว่า สถาบันการเงินขนาดใหญ่และขนาดกลางส่วนใหญ่เห็นว่า หน่วยงานกำกับดูแลไม่มีความจำเป็นต้องกำหนดหลักเกณฑ์การกำกับดูแลความเป็นอิสระของ DPO เพิ่มเติม เนื่องจากสถาบันการเงินมีกระบวนการ Check and Balance เป็นจำนวนมากตามประกาศของธนาคารแห่งประเทศไทยที่มีอยู่แล้ว เช่น นโยบายและกระบวนการแจ้งเบาะแสภายในสถาบันการเงิน หรือการรายงานเมื่อสถาบันการเงินมีการเปลี่ยนแปลงผู้ปฏิบัติงานในฐานะ 2nd Line of Defense ต่อ ธปท. ในทางตรงกันข้ามผู้ให้สัมภาษณ์ของสถาบันการเงินขนาดเล็กซึ่งในทางปฏิบัติอาจไม่ได้การประสานงานกับหน่วยงานกำกับดูแลอย่างใกล้ชิดนั้น เห็นด้วยกับการกำหนดให้สถาบันการเงินมีหน้าที่แจ้งการแต่งตั้งและการเปลี่ยนแปลง DPO ขององค์กรต่อหน่วยงานกำกับดูแล เพื่อให้หน่วยงานกำกับดูแลติดตามประสานงานการทำงานของ DPO และเป็นหลักประกันความเป็นอิสระของ DPO อีกชั้นหนึ่ง

เมื่อสถาบันการเงินแต่ละแห่งมีการกำหนดโครงสร้างกระบวนการทำงานที่ส่งเสริมความเป็นอิสระของ DPO ทำให้ในอนาคตจะมีการเปลี่ยนแปลง DPO โดยไม่ว่าบุคคลนั้นจะเป็นบุคคลภายในสถาบันการเงินหรือบุคคลภายนอก บุคคลนั้นย่อมสามารถใช้ดุลพินิจปฏิบัติหน้าที่ในตำแหน่ง DPO ได้มีอิสระ และในกรณีที่สถาบันการเงินทำการประมวลผลข้อมูลส่วนบุคคลของ DPO โดยมิชอบด้วยกฎหมายย่อมไม่เกิดปัญหาความขัดแย้งทางผลประโยชน์ เนื่องจากสามารถแยกแยะตัวตนในฐานะพนักงานขององค์กรที่เป็น DPO กับตัวตนในฐานะเจ้าของข้อมูลส่วนบุคคลได้

6.1.2 ปัญหาทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย

ในการทำความเข้าใจกระบวนการประมวลผลและดูแลตรวจสอบให้การคุ้มครองข้อมูลส่วนบุคคลขององค์กรเป็นไปตามกฎหมายอย่างครบถ้วน DPO จำเป็นต้องได้รับการสนับสนุนทรัพยากรในด้านต่างๆ ที่จำเป็นและเพียงพอ การได้รับทรัพยากรเช่นนี้ยังส่งผลโดยตรงต่อประเด็นความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO ด้วย จากการสัมภาษณ์พบว่าไม่ว่า DPO ของสถาบันการเงินขนาดใหญ่ ขนาดกลาง หรือขนาดเล็ก ล้วนมีความต้องการหลักๆ ในด้านบุคลากร และด้านเครื่องมือเทคโนโลยีที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานการรักษาความมั่นคง

ปลอดภัยของข้อมูล สิ่งที่แตกต่างกันคือ หากภายหลังกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ สถาบันการเงินขนาดใหญ่และสถาบันการเงินขนาดกลางอาจจะสามารถให้ทุ่มเททรัพยากรบุคคลและเครื่องมือต่างๆ ให้แก่งานด้านข้อมูลส่วนบุคคลได้มากกว่าสถาบันการเงินขนาดเล็ก เนื่องจากมีบุคลากรโดยเฉพาะอย่างยิ่งผู้ที่มีความรู้ความเข้าใจการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีจำนวนน้อยกว่าสถาบันการเงินขนาดใหญ่และขนาดกลาง อีกทั้งสถาบันการเงินขนาดเล็กมีข้อจำกัดว่าระบบบริหารจัดการข้อมูลมักจะถูกจัดทำขึ้นที่ต่างประเทศ ทำให้ยากต่อการเปลี่ยนแปลงแก้ไขให้เป็นไปตามกฎหมาย

6.1.3 ปัญหามาตรฐานการทบทวนการประมวลผลข้อมูลส่วนบุคคลขององค์กร

เนื่องจากในปัจจุบันร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพียงแต่กำหนดมาตรฐานในการตรวจสอบด้านการคุ้มครองข้อมูลส่วนบุคคลที่จะต้องผ่านความเห็นชอบจากคณะกรรมการฯ ว่ามีรายการในการตรวจสอบขั้นต่ำในเรื่องใดบ้าง[7] อย่างไรก็ดี มาตรฐานของสถาบันการเงินยังขาดความชัดเจนเกี่ยวกับรายละเอียดการจัดทำมาตรฐานการทบทวนการปฏิบัติงานให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน ซึ่งประเด็นดังกล่าวเป็นเรื่องที่ สคส. จะต้องให้ความสำคัญอย่างเร่งด่วนเนื่องจากมีความสำคัญต่อการลงทุนพัฒนากระบวนการคุ้มครองข้อมูลส่วนบุคคลของสถาบันการเงินประเทศไทยแต่ละแห่งเป็นอย่างมาก โดยจากการสำรวจพบว่าปัจจุบันสถาบันการเงินขนาดใหญ่เริ่มมีการรับฟังความคิดเห็นของหน่วยธุรกิจและฝ่ายงานที่เกี่ยวข้องภายในองค์กร ขณะที่สถาบันการเงินขนาดกลางขนาดเล็กส่วนใหญ่ในปัจจุบันอาจจะยังไม่มีความเคลื่อนไหวใดๆ มากไปกว่าการตรวจสอบความพร้อมของการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในเบื้องต้นว่ามีการดำเนินการตรวจสอบตามรายการข้างต้นหรือไม่

6.2 ข้อเสนอแนะ

เพื่อให้ DPO ในสถาบันการเงินมีโครงสร้างการปฏิบัติหน้าที่ที่มีความเป็นอิสระ พร้อมทั้งสามารถทำหน้าที่ให้คำแนะนำ ตรวจสอบกระบวนการประมวลผล และกำกับดูแลมาตรการรักษา

[7] ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล หมวด 3 ข้อ 2.5. โปรดดู https://sites.google.com/view/pdpa-2019/pdpa-home#h.oumiepibq8he

ความปลอดภัยของข้อมูลส่วนบุคคลขององค์กรเป็นประโยชน์ต่อการดำเนินธุรกิจขององค์กรควบคู่ไปกับการปฏิบัติตามกฎหมายได้อย่างมีประสิทธิภาพและประสิทธิผล ผู้เขียนมีข้อเสนอแนะดังต่อไปนี้

(1) DPO เป็นผู้ปฏิบัติงานในฐานะ 2nd Line of Defense

หากสถาบันการเงินแต่งตั้ง DPO จากพนักงานภายในองค์กร ควรเป็นที่ปฏิบัติงานในฐานะ 2nd Line of Defense กล่าวคือ ไม่มีธุรกิจหรือส่วนร่วมในการบริหารงานหรือไม่มีผลประโยชน์เกี่ยวข้องกับสถาบันการเงิน หรือไม่มีลักษณะอื่นใดที่ทำให้ไม่สามารถให้ความเห็นตัดสินใจ หรือลงมติเกี่ยวกับการดำเนินงานของสถาบันการเงินได้อย่างเป็นอิสระ

(2) การกำหนดโครงสร้างค่าตอบแทน

โครงสร้างค่าตอบแทนของ DPO จะต้องสะท้อนหน้าที่และความรับผิดชอบของผู้ทำหน้าที่กำกับดูแลการใช้ข้อมูลส่วนบุคคล และไม่ผูกโยงกับผลกำไรหรือเป้าหมายทางธุรกิจของสถาบันการเงิน ตลอดจนมีการติดตามและประเมินประสิทธิภาพและประสิทธิผลของโครงสร้างค่าตอบแทนเป็นระยะ

(3) การรายงานเรื่องข้อมูลส่วนบุคคลต่อผู้บริหารระดับสูง

DPO ควรดูแลให้มีการจัดทำรายงานการประชุมของคณะกรรมการกำกับดูแลข้อมูลของสถาบันการเงินที่มีเนื้อหาครบถ้วน โดยระบุการให้ความเห็นที่สำคัญของกรรมการเป็นรายบุคคลเพื่อพิจารณาประเด็นที่สำคัญ เช่น แผนการดำเนินงานด้านข้อมูลส่วนบุคคล ความเปลี่ยนแปลงของกฎหมายคุ้มครองข้อมูลส่วนบุคคล จำนวนและสาระสำคัญของข้อร้องเรียนของเจ้าของข้อมูลส่วนบุคคล เหตุละเมิดข้อมูลส่วนบุคคล ฯลฯ

นอกจากนี้ สถาบันการเงินจะต้องกำหนดนโยบายและกระบวนการแจ้งเบาะแสการละเมิดข้อมูลส่วนบุคคลภายในองค์กรอย่างเหมาะสม รวมทั้งมาตรการคุ้มครองผู้แจ้งเบาะแสหรือร้องเรียนโดยคำนึงถึงการรักษาความลับเพื่อให้มั่นใจว่าผู้แจ้งเบาะแสหรือร้องเรียนได้รับการคุ้มครองและเพื่อให้มีการดำเนินการโดยไม่ถูกแทรกแซง เช่น การแจ้งเบาะแสหรือร้องเรียนโดยตรงไปยังประธานคณะกรรมการตรวจสอบ หรือกรรมการอิสระ หรือหัวหน้าหน่วยงานตรวจสอบภายใน

(4) การทบทวนตำแหน่ง DPO ในสถาบันการเงิน

สถาบันการเงินอาจไม่มีความจำเป็นต้องกำหนดระยะเวลาหรือวาระการดำรงตำแหน่งไว้ตายตัว แต่ควรกำหนดให้มีการประเมินประสิทธิภาพและประสิทธิผลของการปฏิบัติหน้าที่ DPO อย่างต่อเนื่อง เพื่อให้ไม่เกิดความหละหลวมการปฏิบัติหน้าที่ เช่น วิธีประเมินตนเอง (Self-

Evaluation) วิธีประเมินแบบไขว้ (Cross-Evaluation) หรือการประเมินโดยผู้ประเมินภายนอก (Third-Party Evaluation) อีกทั้งสถาบันการเงินควรมีหน้าที่แจ้งการแต่งตั้งหรือการเปลี่ยนแปลง DPO ขององค์กร พร้อมเหตุผลประกอบการแต่งตั้งหรือการเปลี่ยนแปลงนั้นมายัง ธปท. และ สคส.

(5) ความขัดแย้งทางผลประโยชน์

สถาบันการเงินควรกำหนดนโยบายเรื่องการกำกับดูแลข้อมูลที่ดีให้มีความชัดเจนเป็นลายลักษณ์อักษร โดยนโยบายดังกล่าวจะต้องคำนึงถึงผู้มีส่วนได้เสียทุกฝ่าย (Stakeholders) อย่างเหมาะสม มีความเป็นธรรมในทางธุรกิจโดยไม่เอารัดเอาเปรียบลูกค้าและประชาชน รวมทั้งกำหนดนโยบายเกี่ยวกับการดูแลความขัดแย้งทางผลประโยชน์ เพื่อไม่ให้เกิดปัญหาความขัดแย้งทางผลประโยชน์ระหว่างบทบาทหน้าที่ DPO ตามกฎหมายกับบทบาทหน้าที่อื่นที่บุคคลซึ่งเป็น DPO มีต่อสถาบันการเงิน นโยบายการกำกับดูแลข้อมูลส่วนบุคคลที่ดีในที่นี้อาจรวมถึงการออกบทบัญญัติเกี่ยวกับจรรยาบรรณทางธุรกิจ และจริยธรรมทางข้อมูล เพื่อเป็นแนวทางปฏิบัติภายในองค์กร เช่น ในกรณีที่ DPO ถูกลงโทษทางวินัยควรมีการจัดตั้งคณะกรรมการสืบสวนข้อเท็จจริงซึ่งไม่มีผู้บริหารอยู่ในองค์คณะ ทำหน้าที่ทบทวนข้อเท็จจริงก่อนดำเนินการลงโทษดังกล่าว

(6) การสืบทอดตำแหน่ง DPO ในสถาบันการเงิน

คณะกรรมการกำกับดูแลข้อมูลของสถาบันการเงินควรดูแลให้เกิดความมั่นใจว่า DPO มีความสามารถในการจัดการงานด้านข้อมูลส่วนบุคคลของสถาบันการเงิน รวมทั้งมีแผนการสืบทอดตำแหน่ง (Succession Plan) สำหรับบุคคลที่จะมาทำหน้าที่เป็น DPO เพื่อให้การดำเนินธุรกิจและการคุ้มครองข้อมูลส่วนบุคคลขององค์กรเป็นไปอย่างต่อเนื่อง

(7) ความรู้ความสามารถของ DPO ในสถาบันการเงิน

สถาบันการเงินควรร่วมกันจัดทำมาตรฐานคุณสมบัติของ DPO ในสถาบันการเงิน เพื่อกำหนดความรู้ความสามารถ ทักษะ รวมถึงคุณสมบัติส่วนบุคคล[8] ของบุคคลที่จะทำหน้าที่ดังกล่าวเป็นเกณฑ์ในการพิจารณาเบื้องต้นแล้วส่งให้ สคส. พิจารณาเพิ่มเติม โดย DPO สถาบันการเงินจะต้อง

[8] Network of Data Protection Officers of the EU institution and bodies, Professional Standards for Data Protection Officers of the EU institution and bodies working under Regulation (EC) 45/2001. Ibid. p.4. (คุณสมบัติส่วนบุคคล (Personal Quality) ที่ DPO พึงมี ได้แก่ ความซื่อสัตย์ ความคิดริเริ่มสร้างสรรค์ ความสามารถในการบริหารจัดการ การใช้ดุลพินิจความสามารถในปรับตัวแม้ในสถานการณ์ที่ยากลำบาก ความสนใจด้านการคุ้มครองข้อมูลส่วนบุคคล และมีแรงจูงใจในการปฏิบัติงานในตำแหน่ง DPO)

มีความรู้ความเข้าใจในด้านต่างๆ ได้แก่ กฎหมาย ความเข้าใจการดำเนินธุรกิจและการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงิน มาตรฐานการรักษาความปลอดภัยข้อมูล เทคโนโลยีและการบริหารจัดการความเสี่ยง นอกจากนี้ DPO มีหน้าที่ให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานภายในองค์กร การฝึกอบรม และย้ำเตือนภาระหน้าที่ความรับผิดชอบขององค์กรที่มีต่อข้อมูลส่วนบุคคลให้แก่ พนักงาน หัวหน้าฝ่ายงาน/ส่วนงาน ผู้บริหาร ผู้จัดการ และกรรมการของสถาบันการเงินตระหนักรู้ถึงมาตรการปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยสถาบันการเงินอาจจัดให้มีการฝึกอบรม สัมมนาแก่พนักงานทุกคน รวมถึงจัดสอบวัดระดับความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ปฏิบัติงานด้านดังกล่าวเป็นประจำ

บรรณานุกรม

ตัวบทกฎหมาย

General Data Protection Regulation (GDPR)

แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การกำกับดูแลข้อมูล (Data Governance)

ประกาศธนาคารแห่งประเทศไทยที่ สกส. 1/2561 เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct)

ประกาศธนาคารแห่งประเทศไทยที่ สกส. 12/2562 ธรรมาภิบาลของสถาบันการเงินเฉพาะกิจ

ประกาศธนาคารแห่งประเทศไทยที่ สนส. 3/2564 เรื่อง หลักเกณฑ์การพิจารณาให้ความเห็นชอบการแต่งตั้งกรรมการ ผู้จัดการ ผู้มีอำนาจในการจัดการ หรือที่ปรึกษาของสถาบันการเงิน บริษัทแม่ของสถาบันการเงิน และบริษัทลูกที่ประกอบธุรกิจทางการเงิน

ประกาศธนาคารแห่งประเทศไทยที่ สนส. 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing) ในการประกอบธุรกิจของสถาบันการเงิน

ประกาศธนาคารแห่งประเทศไทยที่ สนส. 10/2561 ธรรมาภิบาลของสถาบันการเงิน

ประกาศธนาคารแห่งประเทศไทยที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีบันทึกรายการกิจกรรมประมวลผล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วน

บุคคล

ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หนังสือภาษาไทย

ปิยะบุตร บุญอร่ามเรือง, พีรพัฒ โชคสุวัฒนสกุล, ปิติ เอี่ยมจำรูญลาภ, ชวิน อุ่นภัทร และ ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล. Thailand Data Protection Guideline 2.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย: ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2562.

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. Thailand Data Protection Guildlines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Version 3.0 Extension). โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย: 2564.

สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน). มาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขา Digital security and privacy. 2564.

————. ร่างมาตรฐานอาชีพและคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขา Digital security and privacy. 2564.

สมาคมธนาคารไทย. แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร สมาคมธนาคารไทย (Guideline on Personal Data Protection for Thai Banks). 2564.

บทความภาษาไทย

กลุ่มงานมาตรฐานด้านการตรวจสอบภายใน. แนวปฏิบัติการตรวจสอบภายใน [ออนไลน์]. 2546. แหล่งที่มา: http://www.khonkaen.go.th/auditor/admin/interest_file/102127_536.pdf [เข้าถึงเมื่อ 21 ตุลาคม 2563]

กุลโมไนย พิทักษ์โชติไชย. มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสถาบันการเงิน. หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยเกริก: 2556.

ดร.ปริญญา หอมเอนก. 10 แนวโน้ม Cybersecurity and Privacy Trends 2020 [ออนไลน์]. 2563. แหล่งที่มา: https://www.bangkokbiznews.com/blog/detail/649796 [เข้าถึงเมื่อ 21 ตุลาคม 2563]

ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. เอกสารประกอบการสัมภาษณ์เรื่อง DPO Competency Framework and Training Roadmap. 2564.

ตลาดหลักทรัพย์แห่งประเทศไทย. กรอบการบริหารความเสี่ยงองค์กร (ERM Framework) [ออนไลน์]. 2014. แหล่งที่มา: https://www.set.or.th/th/about/overview/files/Risk_2015_v2.pdf [เข้าถึงเมื่อ 20 ตุลาคม 2563]

สำนักงานคณะกรรมการนโยบายวิทยาศาสตร์เทคโนโลยีและนวัตกรรมแห่งชาติ. คู่มือป้องกันผลประโยชน์ทับซ้อน (Conflict of Interest). 2561.

หนังสือภาษาต่างประเทศ

COSO. LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE. The Institute of Internal Auditors (IIA), 2015.

Douwe Korff, and Marie Georges. The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation [Online]. 2019. Available from: https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf [22 Jan 2021].

Thomas Shaw. DPO Handbook Data Protection Officers Under the GDPR. Second edition. The International Association of Privacy Professionals (IAPP), 2018.

บทความต่างประเทศ

Article 29 Data Protection Working Party (WP29). Guidelines on consent under Regulation 2016/679 [Online]. 2017 (As last Revised and Adopted on 10 April 2018). Available from: https://ec.europa.eu/newsroom/article29/items/623051/en [21 Jan 2021].

———. 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 [Online]. 2017. Available from:

https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 [20 Jan 2021].

———. Guidelines on Data Protection Officers ('DPOs') [Online]. 2017. Available from: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A [20 Jan 2021].

———. Opinion 15/2011 on the definition of consent [Online]. 2011. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf [24 Oct 2021].

———. Statement on the role of a risk-based approach in data protection legal frameworks [Online]. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf [3 Nov 2021].

Bart Custers, and Helena U Vrabec. Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection [Online]. 2016. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046774 [1 Nov 2021].

Centre for Information Policy Leadership (CIPL). Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation [Online]. 2016. Available from: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/11/final_cipl_gdpr_dpo_paper_17_november_2016.pdf [17 Oct 2020].

———. The Role and Function of a Data Protection Officer in Practice and in the European Commission's Proposed General Data Protection Regulation : Report on DPO Survey Results [Online]. 2013. Available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf [14 Jan 2021].

CMS. GDPR Enforcement Tracker [Online]. 2021. Available from: https://www.enforcementtracker.com/?insights [30 Oct 2021].

CNIL. Guide de Correspondant Informatique et Libertés [Online]. 2011. Available from:

https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf [25 Oct 2021].

DPEXNetwork. Issues and Challenges faced by Data Protection Officers in Singapore (Part I) [Online]. 2020. Available from: https://www.dpexnetwork.org/articles/issues-and-challenges-faced-data-protection-officers-singapore-part-i/ [28 Jan 2564].

EDPS. Position of the DPO in the organigramme [Online]. Available from: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en [17 Jan 2021].

———. Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 [Online]. Available from: https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf [7 Jan 2021].

———. Position paper on the role of Data Protection Officers of the EU institutions and bodies [Online]. 2018. Available from: https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf [16 Jan 2021].

———. Preliminary Opinion on privacy by design (Opinion 5/2018) [Online]. 2018. Available from: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf [22 Oct 2021].

Eric Lachaud. DPO certification should be monitored. SSRN Electric Journal (January, 2018).

European Commission. Adequacy decisions [Online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [27 Sep 2021].

FERMA-ECIIA. GDPR & Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation [Online]. 2019. Available from: https://www.ferma.eu/advocacy/gdpr-corporate-governance-the-role-of-internal-audit-and-risk-management-one-year-after-implementation/ [12 Oct 2020].

———. Guidance on the 8th EU Company Law Directive - Article 41 [Online]. 2010. Available from: https://www.iia.nl/SiteFiles/ECIIA%20FERMA.pdf [13 Mar 2021].

Garante per la Protezione dei Dati Personali. FAQs on DPO [Online]. Available from: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793 [20 Jan 2021].

IAPP-EY. IAPP-EY Annual Privacy Governance Report 2019 [Online]. Available from: https://iapp.org/store/books/a191P000003Qv5xQAC/ [16 Nov 2020].

IAPP. Get DPO Ready: Training and Resources [Online]. 2018. Available from: https://iapp.org/train/Data-protection-training/ [20 Jan 2021].

ICO. How do we apply legitimate interests in practice? [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ [2 Nov 2021].

———. Manifestly unfounded and excessive requests [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/ [30 Oct 2021].

Network of Data Protection Officers of the EU institution and bodies. Professional Standards for Data Protection Officers of the EU institution and bodies working under Regulation (EC) 45/2001. 2010.

OECD. Good Practice Principles for Data Ethics in the Public Sector [Online]. Available from: https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf [31 Oct 2021].

PDPC Singapore. DPO Competency Framework and Training Roadmap [Online]. 2019. Available from: https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap/Competencies#dpm [21 Oct 2563].

Ryerson University. GUIDELINES FOR MANAGING REAL, POTENTIAL, AND PERCEIVED CONFLICTS OF INTEREST [Online]. 2017. Available from: https://www.ryerson.ca/content/dam/research/documents/ethics/guidelines-for-managing-real-potential-and-perceived-conflicts-of-interest.pdf [17 Jan 2564].

The Institution of Internal Auditors. IAA Position Paper - The Three Lines of Defense in Effective Risk Management and Control [Online]. January 2013. Available from:

https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf [11 Mar 2021].

US Federal Information Processing Standards (FIPS) Publication 1999. Standards for Security Categorization of Federal Information and Information Systems [Online]. 2004. Available from: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf [2 Nov 2021].

การสัมภาษณ์

กลุ่มเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากสถาบันการเงิน 13 แห่ง. "สัมภาษณ์ เรื่อง บทบาทหน้าที่และปัญหาที่เกิดขึ้นจากการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล." ระหว่างเดือนมิถุนายน - สิงหาคม 2564.

ดร.สุนทรีย์ ส่งเสริม นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. "สัมภาษณ์ เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล." 29 กรกฎาคม 2564.

วีระ ประเสริฐนุกูล ผู้ช่วยผู้อำนวยการฝ่ายบริหารความเสี่ยงภาพรวม ธนาคารแห่งประเทศไทย. "สัมภาษณ์ เรื่อง บทบาทหน้าที่และปัญหาที่เกิดขึ้นจากการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล." 6 สิงหาคม 2564.

ประวัติผู้เขียน

ชื่อ-สกุล	อริยะ ตังสวานิช
วัน เดือน ปี เกิด	10 สิงหาคม 2538
สถานที่เกิด	จังหวัดชลบุรี
วุฒิการศึกษา	พ.ศ.2561 สำเร็จการศึกษาในระดับปริญญาตรี หลักสูตรนิติศาสตรบัณฑิต จากคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ พ.ศ.2562 เข้าศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิต หมวดวิชากฎหมายเอกชนและธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย พ.ศ.2562 สำเร็จเนติบัณฑิต เนติบัณฑิตยสภา สมัยที่ 72
ที่อยู่ปัจจุบัน	68/26 ม.2 ต.บ้านสวน อ.เมืองชลบุรี จ.ชลบุรี 20000