วารสารนิติศาสตร์
มหาวิทยาลัยธรรมศาสตร์
THAMMASAT LAW JOURNAL

ชื่อเรื่อง: คำถามที่ต้องการคำตอบในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ชื่อผู้แต่ง: ชวิน อุ่นภัทร

การอ้างอิงที่แนะนำ: ชวิน อุ่นภัทร, “คำถามที่ต้องการคำตอบในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,” วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ปีที่ 49, ฉบับที่ 1, 148 (2563)

โครงการวารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ เลขที่ 2 ถนนพระจันทร์ แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพมหานคร 10200 โทร. 02 613 2169 อีเมล tu.lawjournal@tu.ac.th

ปกิณกะกฎหมาย

คำถามที่ต้องการคำตอบในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
Mysteries in the Personal Data Protection Act B.E. 2562 (2019)

ชวิน อุ่นภัทร*
อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
Chawin Ounpat
Lecturer, Faculty of Law, Thammasat University

ความนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกที่ใช้เป็นการทั่วไปกับทุกภาคส่วนจากเดิมที่การคุ้มครองข้อมูลส่วนบุคคลนั้นมีอยู่ในบางภาคส่วนที่มีองค์กรกำกับดูแล เช่น ธุรกิจโทรคมนาคมภายใต้การกำกับดูแลของ กสทช. การประกอบธุรกิจธนาคารและสถาบันการเงินที่อยู่ภายใต้กำกับดูแลของธนาคารแห่งประเทศไทย หรือภาคการให้บริการด้านสาธารณสุขที่มีกฎหมายเกี่ยวกับการรักษาความลับหรือข้อมูลผู้ป่วยซึ่งเป็นข้อมูลสุขภาพ เป็นต้น พระราชบัญญัติฉบับนี้ผ่านความเห็นชอบของสภานิติบัญญัติแห่งชาติ (สนช.) เมื่อวันที่ 28 กุมภาพันธ์

* นิติศาสตรบัณฑิต (เกียรตินิยมอันดับหนึ่ง) มหาวิทยาลัยธรรมศาสตร์, LLM (Thesis), Indiana University – University of Oxford Joint Program in Information Law and Policy, SJD Candidate, Indiana University Maurer School of Law.

พ.ศ. 2562 และได้มีการประกาศในราชกิจจานุเบกษาในวันที่ 27 พฤษภาคม พ.ศ. 2562 โดยผลบังคับแบบเต็มรูปแบบจะมีขึ้นเมื่อพ้น 1 ปีนับจากวันถัดจากวันประกาศในราชกิจจานุเบกษาซึ่งได้แก่วันที่ 28 พฤษภาคม พ.ศ. 2563 นั่นเอง กล่าวคือ เหลือเวลาเพียงไม่กี่เดือนเท่านั้นที่กฎหมายฉบับนี้จะมีผลบังคับใช้ ฉะนั้นภาคส่วนต่าง ๆ ไม่ว่าจะภาครัฐหรือภาคเอกชนเองก็กำลังอยู่ในช่วงการเตรียมความพร้อมเพื่อให้การดำเนินการเป็นไปตามกฎหมายฉบับนี้อย่างเร่งด่วน หากไม่สามารถปฏิบัติตามได้ก็จะมีความเสี่ยงในการถูกปรับทางปกครองซึ่งมีอัตราสูงไม่เกิน 1 ล้านบาท 3 ล้านบาท หรือ 5 ล้านบาท แล้วแต่กรณี

ผู้เขียนได้มีโอกาสเข้าไปเป็นที่ปรึกษาในชั้นการพิจารณาของคณะกรรมาธิการซึ่งเป็นคณะกรรมการวิสามัญของ สนช. และยังได้มีโอกาสได้บรรยายให้กับองค์กรต่าง ๆ เกี่ยวกับพระราชบัญญัติดังกล่าวในหลายวาระ พบเห็นปัญหาและอุปสรรคที่อาจจะเกิดขึ้นได้ในอนาคตจากการบังคับใช้กฎหมายฉบับนี้ หลายประเด็นก็ยังเป็นประเด็นที่ไม่อาจหาข้อสรุปได้อย่างแน่ชัด เพราะผู้เขียนเองก็ไม่ใช่ผู้ที่มีอำนาจชี้ขาดในอนาคตอย่างคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่จะเข้ามาเป็นผู้กำกับดูแล (regulator) และบังคับใช้กฎหมายฉบับนี้ หรือศาลซึ่งจะเป็นผู้พิจารณาวินิจฉัยคดีในที่สุด ในข้อเขียนนี้ผู้เขียนจะได้นำเสนอประเด็นและตั้งข้อสังเกตในเรื่องที่อาจจะมีปัญหาในการบังคับใช้พระราชบัญญัติฉบับนี้ในอนาคตรวมถึงประเด็นที่ส่งผลกระทบต่อการปฏิบัติตามกฎหมายของภาคส่วนต่าง ๆ ในลักษณะของ “คำถามที่ต้องการคำตอบ” ซึ่งยังอาจไม่ครอบคลุมเพียงพอ (comprehensive) ที่จะนำเสนอในรูปแบบของบทความทางวิชาการที่สมบูรณ์ แต่เห็นควรที่ได้กล่าวและได้ตั้งข้อสังเกตในบางประเด็นต่อไป

1. คำถามที่ต้องการคำตอบข้อที่หนึ่ง เมื่อใดประกาศของคณะกรรมการจะออกมาเสียที

ในพระราชบัญญัติฉบับนี้ หลายบทมาตราได้กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ประกาศกำหนด จริง ๆ แล้วการให้อำนาจผู้กำกับดูแลในการออกกฎหมายลูกนั้นก็เป็นเรื่องที่พบเห็นได้อยู่ทั่วไปในการกำกับดูแลกิจการประเภทต่าง ๆ ในส่วนของกฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้ก็เช่นเดียวกันได้มีบทมาตราที่ให้อำนาจคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในหลายส่วน เช่น มาตรการปกป้องข้อมูลส่วนบุคคลกรณีการประมวลข้อมูลเพื่อการจัดทำเอกสารประวัติศาสตร์ วิจัยหรือสถิติ (มาตรา 24 (1))[1] หลักเกณฑ์เกี่ยวกับการส่งหรือโอนข้อมูลไปยังต่างประเทศ (มาตรา 28 และ 29) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูล (มาตรา 37(1)) หลักเกณฑ์เกี่ยวกับการแจ้งเมื่อมีเหตุข้อมูลรั่วไหล (breach notification) (มาตรา 37(4)) การประกาศหลักเกณฑ์หรือประเภทผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41) เป็นต้น หลักเกณฑ์ต่าง ๆ เหล่านี้มีความจำเป็นต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในระดับที่แตกต่างกัน

[1] ต่อไปนี้เลขมาตราที่อ้างอิง หากมิได้ระบุไว้เป็นอย่างอื่นให้หมายถึงเลขมาตราของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กรอบเวลาที่กฎหมายกำหนดสำหรับการออกหลักเกณฑ์ในรูปแบบประกาศเหล่านี้ได้กำหนดไว้ในมาตรา 96 ซึ่งกำหนดให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ อย่างไรก็ดีกรอบเวลาดังกล่าวเป็นเพียงระยะเวลาเร่งรัด มิได้มีบทลงโทษในกรณีไม่สามารถดำเนินการให้แล้วเสร็จ เนื่องจากกฎหมายกำหนดว่าหากไม่สามารถดำเนินการให้แล้วเสร็จได้ภายใต้กรอบเวลาดังกล่าว รัฐมนตรีจะต้องรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบเท่านั้น

สำหรับความคืบหน้าในปัจจุบันนั้น เมื่อวันที่ 10 ตุลาคม พ.ศ. 2562 ได้มีการเปิดตัวสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)[2] ในขณะที่ปัจจุบันก็ยังอยู่ในขั้นตอนของการสรรหาตัวบุคคลที่จะเข้ามาเป็นคณะกรรมการคุ้มครองส่วนบุคคลที่จะเป็นผู้กำกับดูแลและบังคับใช้กฎหมายฉบับนี้ และยังไม่แน่ชัดว่ากระบวนการสรรหาและแต่งตั้งดังกล่าวจะแล้วเสร็จเมื่อใด ดังนั้นในช่วงที่ตั้งคณะกรรมการแล้ว กฎหมายใช้บังคับแล้ว แต่ประกาศของคณะกรรมการยังไม่ออกน่าจะเป็นช่วงที่มีคำถามเกิดขึ้นมากมายแน่นอนและระยะเวลาเหล่านั้นน่าจะเกิดขึ้นแน่นอน

2. คำถามที่ต้องการคำตอบข้อที่สอง ใครจะเป็นผู้ชี้ขาดและจะมั่นใจได้อย่างไรว่าได้ทำตามกฎหมายฉบับนี้แล้ว

นอกจากการที่ยังไม่มีประกาศคณะกรรมการในหลายเรื่องทำให้ยังไม่มีความแน่ชัดในหลายประเด็นแล้ว หลายประเด็นก็ยังเปิดกว้างให้มีการตีความได้เพราะบทบัญญัติของกฎหมายนั้นเปิดช่องให้เกิดการตีความโดยใช้ถ้อยคำ เช่น การมีมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 ที่จะต้องมีในระดับที่ “เหมาะสม” หรือการประมวลผลข้อมูลส่วนบุคคลโดยอาศัยฐานประโยชน์ที่ชอบธรรม (legitimate interest) ตามมาตรา 24 (5) ซึ่งจะต้องมีการชั่งน้ำหนักกับการคุ้มครองสิทธิและเสรีภาพของบุคคลเพื่อประเมินว่าสามารถอาศัยฐานนี้ในการประมวลผลข้อมูลส่วนบุคคลโดยไม่ต้องอาศัยความยินยอมได้หรือไม่ (legitimate interest assessment: LIA) เป็นต้น ถ้อยคำเหล่านี้ในบางครั้งไม่อาจจะมีการกำหนดให้เห็นอย่างชัดเจนว่ากรณีใดทำได้หรือทำไม่ได้ แล้วสุดท้ายใครจะเป็นผู้ชี้ขาด แน่นอนว่ากลไกตามกฎหมายให้อำนาจคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้กำกับดูแลและบังคับใช้กฎหมายด้วยการลงโทษปรับทางปกครอง อย่างไรก็ดี ในท้ายที่สุดอาจมีกระบวนการอุทธรณ์ไปยังศาลปกครองซึ่งจะเป็นผู้ชี้ขาดในท้ายที่สุด เนื่องจากกฎหมายฉบับนี้เป็นกฎหมายใหม่จึงไม่มีคำพิพากษาที่ใช้เป็นบรรทัดฐานได้เลย สิ่งที่พอจะอ้างอิงได้อาจมีคำอธิบายกฎหมายของต่างประเทศหรือแม้แต่กรณีตัวอย่างที่หน่วยงานกำกับดูแลในต่างประเทศได้บังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับภาคส่วนต่าง ๆ แต่กรณีดังกล่าวก็ไม่อาจจะยืนยันได้อีกว่าผู้กำกับดูแลของไทยหรือแม้กระทั่งศาลจะยึดถือแนวทางดังกล่าวด้วยหรือไม่ แม้กระนั้นเอง หากเรามีข้ออ้างอิงว่าได้ปฏิบัติตามมาตรฐานหรือแนวปฏิบัติของต่างประเทศก็น่าจะเป็นข้อหนึ่งที่จะพอยืนยันได้ว่าเราได้

[2] “ดีอีเอส เปิดตัวสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รองรับข้อกำหนดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ประเดิมกิจกรรมแรกจัดเวที ‘PDPA –Privacy for All’,” รัฐบาลไทย, (2562) สืบค้นเมื่อ วันที่ 5 กุมภาพันธ์ 2563, จาก https://www.thaigov.go.th/news/contents/details/23524.

พยายามปฏิบัติตามกฎหมายฉบับนี้แล้ว เช่น แนวทาง (guidelines) ที่ได้รับการยอมรับในสหภาพยุโรป มาตรฐานสากลที่ได้รับการยอมรับอย่าง ISO หรือแม้แต่แนวปฏิบัติของประเทศไทย (Thailand Data Protection Guideline: TDPG)[3] เป็นต้น อย่างน้อยก็จะสามารถช่วยให้เราพิสูจน์ได้ว่าเราได้มีหลักคิดในการคุ้มครองข้อมูลส่วนบุคคลและได้มีความพยายาม (effort) ในระดับหนึ่งแล้วส่วนจะเพียงพอหรือไม่นั้นก็เป็นประเด็นที่จะต้องพิจารณากันต่อไป

แนวทางหนึ่งที่น่าจะพอเป็นไปได้คือเมื่อมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในช่วงแรก แทนที่จะเป็นผู้บังคับใช้กฎหมายอย่างเคร่งครัด คณะกรรมการน่าจะมีบทบาทเป็นพี่เลี้ยงหรือผู้ที่สามารถให้คำปรึกษาให้แก่หน่วยงานต่าง ๆ ในเรื่องของแนวทางในการปฏิบัติตามกฎหมายที่คณะกรรมการยอมรับเป็นอย่างน้อยในการสร้างความเข้าใจและให้หน่วยงานได้มีโอกาสปรับปรุงกระบวนการปฏิบัติและดำเนินการตามกฎหมายฉบับนี้ได้ น่าจะก่อให้เกิดการปฏิบัติตามกฎหมายได้และเกิดบรรยากาศที่ดีระหว่างผู้กำกับดูแลและผู้อยู่ภายใต้การกำกับดูแลเอง นอกจากนั้นแนวในกรณีที่ภาคส่วนนั้นมีผู้กำกับดูแลอยู่เดิมแล้ว คณะกรรมการก็ควรจะได้ร่วมมือกับผู้กำกับดูแลภาคส่วนนั้น ๆ เพื่อพิจารณาถึงลักษณะเฉพาะของภาคส่วนนั้นประกอบด้วย หลังจากนั้นจึงค่อยดำเนินการบังคับตามกฎหมายอย่างเคร่งครัดต่อไป

3. คำถามที่ต้องการคำตอบข้อที่สาม บทบัญญัติที่คลาดเคลื่อนจะใช้บังคับในทิศทางใดในอนาคต

บทบัญญัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นหลายบทมาตราเรียกได้ว่านำมาจากบทบัญญัติของ GDPR เป็นส่วนใหญ่ โดยจะมีบางส่วนที่แตกต่างไปจาก GDPR อย่างไรก็ดีหลายบทมาตราได้รับเอามาแล้วมีข้อผิดพลาดบางประการทำให้ข้อความตามกฎหมายไทยนั้นมีความคลาดเคลื่อนอันอาจจะทำให้เกิดปัญหาในการบังคับใช้ต่อไปหากเรายึดติดที่ถ้อยคำตัวอักษรและอาจมีความจำเป็นในอนาคตที่จะต้องแก้ไขกฎหมายให้ถูกต้องเหมาะสมในโอกาสต่อไป

ตัวอย่างแรกสำหรับบทบัญญัติที่คลาดเคลื่อน ได้แก่ มาตรา 41 ที่ว่าด้วยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (data protection officer: DPO) ซึ่งได้กำหนดประเภทของหน่วยงานองค์กรที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในมาตรา 41 (3) นั้นกำหนดให้ กรณีกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว[4] ซึ่ง

---

[3] ปิยะบุตร บุญอร่ามเรือง และคณะ, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines 2.0), (กรุงเทพ: ศูนย์วิจัยกฎหมายและการพัฒนา จุฬาลงกรณ์มหาวิทยาลัย, 2562).

[4] ประเภทข้อมูลส่วนบุคคลตามมาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด.

มาตรานี้ได้นำมาจาก Article 37(1)(C)[5] ของ GDPR ซึ่งถ้าเปรียบเทียบกันดูแล้วจะเห็นว่าถ้อยคำที่ไม่ปรากฏในกฎหมายไทยได้แก่การประมวลผลข้อมูลส่วนบุคคลจำนวนมาก (large scale) การประมวลผลข้อมูลจำนวนมากนี้มีตัวอย่างอยู่ใน Guidelines on Data Protection Officers ได้แก่ การประมวลผลข้อมูลคนไข้ในโรงพยาบาล การประมวลผลข้อมูลของธนาคารและบริษัทประกัน หรือการประมวลผลข้อมูลของผู้ประกอบการโทรคมนาคมหรือผู้ให้บริการอินเทอร์เน็ต (internet service providers) ส่วนตัวอย่างที่ไม่เป็นการประมวลผลข้อมูลจำนวนมาก เช่น การประมวลผลข้อมูลคนไข้ของหมอส่วนตัว (individual physician) หรือการประมวลผลข้อมูลอาชญากรรมของทนายความส่วนตัว (individual lawyer)[6] เป็นต้น กรณีนี้ก็จะเห็นได้ว่าตามกฎหมายไทยมาตรา 41(3) มิได้ให้อำนาจคณะกรรมการประกาศกำหนดเหมือนอย่างมาตรา 41 (1) และ (2) แต่อย่างใด ทำให้เมื่อกิจกรรมหลัก (core activities)[7] เป็นการประมวลผลข้อมูลอ่อนไหวแล้ว ไม่ว่าจะเป็นการประมวลผลข้อมูลจำนวนมากหรือไม่ เช่นนี้ก็จะต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฉะนั้นกรณีของหมอส่วนตัวหรือหมอที่มีคลินิกขนาดเล็กและมีฐานลูกค้าจำนวนน้อยก็จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย เพราะกฎหมายไม่ได้มีข้อกำหนดเรื่องการประมวลผลข้อมูลจำนวนมากแต่อย่างใด ซึ่งอาจจะไม่ชอบด้วยเหตุผลนักที่จะกำหนดให้กรณีดังกล่าวต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างถัดมา คือ มาตรา 25 วรรค 1 ซึ่งเป็นบทบัญญัติที่กำหนดข้อห้ามมิให้เก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง โดยมีข้อยกเว้นคือความยินยอม (มาตรา 25 วรรค 1(1)) และเหตุที่จะได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 และมาตรา 26 (มาตรา 25 วรรค 1(2)) จะเห็นได้ว่าข้อยกเว้นเหล่านี้ต่างก็ย้อนกลับไปพิจารณาฐานทางกฎหมายตามมาตรา 24 และมาตรา 26 แล้วแต่กรณี ดังนี้ย่อมสังเกตได้ว่าสุดท้ายกฎหมายก็อนุญาตให้เก็บรวบรวมข้อมูลจากแหล่งอื่นได้หากมีฐานเป็นความยินยอมหรือฐานอื่นที่ไม่ใช่ความยินยอม และต้องกลับไปพิจารณามาตรา 24 และมาตรา 26 ในที่สุด ใน GDPR เองก็มิได้มีบทห้ามการเก็บรวบรวมข้อมูลจากแหล่งอื่น การเขียนมาตรา 25 จึงเป็นข้อความที่ไม่ได้มีความจำเป็นที่จะต้องบัญญัติซ้ำกับมาตรา 24 และมาตรา 26 อีกต่อไป ถัดมาในมาตรา 25 วรรค 2 ก็ยังอาจทำให้เข้าใจผิดไปอีก เพราะถ้อยคำของมาตรา 25 วรรค 2 นั้นกำหนดให้ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอม

---

[5] The General Data Protection Regulation (EU) 2016/679 (GDPR), Article 31(1)(C) “the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.”

[6] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (‘DPOs’), 2017, p.21.

[7] กิจกรรมหลัก (core activities) หมายถึง กิจกรรมที่เป็นการดำเนินการหลัก (key operations) เพื่อให้บรรลุวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี เช่น การประมวลผลข้อมูลคนไข้ของโรงพยาบาลที่มีกิจกรรมหลักคือการดำเนินการเพื่อรักษาคนไข้ เป็นต้น แต่กิจกรรมเสริมประการอื่น (support functions หรือ ancillary functions) เช่น ฝ่ายบุคคลของโรงพยาบาล หรือฝ่าย IT ของโรงพยาบาล เช่นนี้ไม่ถือเป็นกิจกรรมหลักของโรงพยาบาล เป็นต้น โปรดดู ibid, p.20.

ตามวรรคหนึ่งโดยอนุโลม ข้อความเช่นนี้ย่อมชวนทำให้เข้าใจผิดว่าหน้าที่ในการแจ้งนั้นจะใช้เฉพาะกับการเก็บข้อมูลจากแหล่งอื่นที่ต้องได้รับความยินยอมเท่านั้น ซึ่งจริง ๆ แล้วไม่เป็นเช่นนั้น เพราะหากตีความว่าหน้าที่ในการแจ้งตามมาตรา 25 นั้นใช้เฉพาะกรณีที่ข้อมูลต้องได้รับความยินยอมเท่านั้น มาตรา 25 วรรค 2 ที่เป็นข้อยกเว้นกรณีที่ไม่ต้องแจ้งจะไม่มีที่ใช้ ฉะนั้นมาตรา 25 วรรค 2 ที่เป็นหน้าที่แจ้งเจ้าของข้อมูลเมื่อรับมาจากแหล่งอื่นนั้น ผู้ควบคุมข้อมูลจะต้องแจ้งไม่ว่าฐานในการเก็บรวมรวมนั้นจะเป็นฐานใดก็ตามเว้นแต่เข้าข้อยกเว้นที่ไม่ต้องแจ้งดังที่จะได้กล่าวถัดไป

นอกจากในวรรคแรกจะมีข้อสังเกตดังที่ได้กล่าวมาข้างต้นแล้ว วรรค 2 ก็เป็นบทบัญญัติที่คลาดเคลื่อนด้วยเช่นกัน มาตรา 25 วรรค 2 เป็นเรื่องข้อยกเว้นการแจ้งเจ้าของข้อมูลส่วนบุคคลในกรณีที่ได้รับข้อมูลมาจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง มาตรา 25 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลในกรณีที่รับข้อมูลมาจากแหล่งอื่น เว้นแต่มีกรณีที่ไม่ต้องแจ้งตามมาตรา 25 วรรค 2 (1)-(4) มาตรานี้กฎหมายไทยได้รับมาจาก Article 14(5)[8] ของ GDPR ซึ่งกำหนดข้อยกเว้นไว้ 4 กรณีเช่นเดียวกับมาตรา 25 วรรค 2 บทบัญญัติที่น่าจะมีความคลาดเคลื่อนได้แก่ มาตรา 25 วรรค 2 (2) ซึ่งกำหนดให้ไม่ต้องมีการแจ้งเจ้าของข้อมูลส่วนบุคคลหากการแจ้งไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล ส่วนใน Article 14(5)(b) มีกรณียกเว้นได้แก่ การแจ้งนั้นไม่อาจทำได้เพราะเป็นไปไม่ได้ (impossible) หรือการแจ้งจะเป็นภาระอันเกินควร (disproportionate effort) หรือการแจ้งจะเป็นอุปสรรคต่อวัตถุประสงค์ของการประมวลผลข้อมูลนั้นอย่างยิ่ง (serious impairment of objectives) จะเห็นได้ว่าถ้อยคำที่ใช้ก็คลาดเคลื่อนไปส่วนหนึ่งซึ่งก็อาจมีผลต่อการบังคับกฎหมายข้อนี้ต่อไป นอกจากนี้ในส่วนที่คลาดเคลื่อนเป็นอย่างมากได้แก่ มาตรา 25 วรรค 2 (3) ที่กฎหมายกำหนดให้ไม่ต้องมีการแจ้งหากการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ส่วน GDPR ที่เป็นต้นแบบของมาตรานี้คือ Article 14(5)(C) ที่กำหนดให้การได้มาซึ่งข้อมูลหรือการเปิดเผยเป็นที่ที่กฎหมายกำหนดไว้โดยชัดแจ้ง (obtaining or disclosure is expressly laid down by law) จะเห็นได้ว่าความคลาดเคลื่อนนี้คำที่สำคัญคือ expressly ซึ่งแปลได้ว่าเป็นการกำหนดไว้โดยชัดแจ้งตามกฎหมายอยู่แล้วจึงไม่ต้องไปแจ้งเจ้าของข้อมูลอีก แต่ในกฎหมายไทยกลับเขียนว่าไม่ต้องแจ้งหากเป็นเรื่องที่ต้องทำตามกฎหมายกำหนดอย่างเร่งด่วนซึ่งไม่ตรงกับถ้อยคำในภาษาอังกฤษมาก ตัวอย่างกรณีนี้ ได้แก่

---

[8] GDPR, Article 14 (5) "Paragraphs 1 to 4 shall not apply where and insofar as:

...

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or ...".

กรณีที่หน่วยงานเก็บภาษีมีหน้าที่ตามกฎหมายที่จะต้องได้รับข้อมูลรายได้ลูกจ้างมาจากนายจ้าง การได้มาซึ่งข้อมูลดังกล่าวมิใช่การได้มาซึ่งข้อมูลจากเจ้าของข้อมูลโดยตรงจึงอยู่ในบังคับของ Article 14 แต่เนื่องจากหน้าที่ดังกล่าวเป็นสิ่งที่กฎหมายได้กำหนดไว้อย่างชัดแจ้งจึงไม่จำเป็นที่จะต้องแจ้งลูกจ้างซึ่งเป็นเจ้าของข้อมูลอีกแต่อย่างใด[9] เป็นต้น แต่เมื่อพิจารณาจากมาตรา 25 วรรค 2 (3) ในถ้อยคำที่ใช้แล้ว กรณีดังกล่าวจะเป็นเรื่องเร่งด่วนที่ได้รับยกเว้นหรือไม่ จะเห็นว่าอาจจะไม่ใช่ในทุกกรณี

4. คำถามที่ต้องการคำตอบข้อที่สี่ ผู้ประกอบการและภาคส่วนต่าง ๆ จะรับมือและเตรียมพร้อมในการปฏิบัติตามกฎหมายฉบับนี้อย่างไร

ภายใต้สถานการณ์ที่หลายเรื่องยังไม่ชัดเจนนี้เราจะทำอย่างไรคงเป็นข้อที่สำคัญเพราะในเดือนพฤษภาคมที่จะถึงนี้กฎหมายฉบับนี้จะได้ใช้บังคับแล้ว ประเด็นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น เราจะต้องเข้าใจว่าสิ่งที่กฎหมายต้องการกำกับคือการเก็บรวบรวม ใช้และเปิดเผยข้อมูล หรือที่ทาง GDPR ใช้คำรวม ๆ ว่าการประมวลผลข้อมูลส่วนบุคคล (processing)[10] กิจกรรมประมวลผลข้อมูลเหล่านี้ (processing activities) จะต้องมีฐานทางกฎหมายรองรับ (lawful basis) เมื่อพิจารณาถึงฐานทางกฎหมายได้แล้วจึงพิจารณาหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต่อไปว่าจะดำเนินการกับข้อมูลส่วนบุคคลเหล่านั้นอย่างไรให้ชอบด้วยกฎหมาย ในการที่จะระบุฐานทางกฎหมายและระบุหน้าที่ความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณีนั้นจำเป็นอย่างยิ่งที่จะต้องรู้ว่าข้อมูลส่วนบุคคลที่มีอยู่นั้นมีอะไรบ้างและมีเส้นทางการไหลเวียนข้อมูล (data flow) อย่างไร ประเด็นนี้เป็นประเด็นที่กฎหมายไม่ได้มีบทบัญญัติที่กำหนดหน้าที่ไว้เลย แต่ในทางปฏิบัติแล้วน่าจะต้องเป็นลำดับแรกในการดำเนินการและก็น่าจะเป็นประการที่ใช้เวลามากพอสมควรโดยเฉพาะอย่างยิ่งองค์กรธุรกิจหรือหน่วยงานอื่นใดที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก จากนั้นจะต้องระบุฐานในการประมวลผลข้อมูลให้ได้ และพิจารณาต่อไปว่ามีหน้าที่ความรับผิดชอบในฐานะผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อไป ที่สำคัญต่อไปจากนั้นใครจะเป็นผู้รับผิดชอบในการดำเนินการต่าง ๆ ข้างต้นและการดำเนินการต่าง ๆ จะต้องได้รับการสนับสนุนจากแผนกหรือฝ่ายต่าง ๆ ในองค์กรอย่างไร

ในองค์กรทั่ว ๆ ไป มักมีข้อมูลส่วนบุคคลหลัก ๆ อยู่ 2 ส่วนใหญ่ ๆ ได้แก่ ข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการและข้อมูลส่วนบุคคลของพนักงานหรือบุคลากรในองค์กร ถ้าเป็นในกรณีของหน่วยงานรัฐก็จะมีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับภารกิจของหน่วยงานนั้น ๆ จากนั้นจึงพิจารณาถึงกิจกรรมที่มีการประมวลผลข้อมูลเหล่านั้นซึ่งโดยปกติในข้อมูลชุดเดียวกันอาจมีวัตถุประสงค์ในการประมวลผลข้อมูลได้หลายวัตถุประสงค์และหลายกิจกรรมเหล่านั้นก็อาศัยฐานในการประมวลผล

---

[9] Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, 2018, p.32-33.

[10] GDPR, Article 4 (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

ข้อมูลที่ไม่เหมือนกัน ดังนั้นการเริ่มต้นปฏิบัติตามกฎหมายนี้น่าจะต้องพิจารณาถึงข้อมูลเหล่านี้ในลำดับต้นโดยพิจารณาถึงฐานการประมวลผลข้อมูล จากนั้นจึงพิจารณาถึงกระบวนการดำเนินการเกี่ยวกับข้อมูลนั้นเพื่อปฏิบัติหน้าที่ต่าง ๆ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี ที่น่าพิจารณาอีกคือจะต้องพิจารณาถึงข้อมูลบางประเภทที่มีความอ่อนไหวและได้รับความคุ้มครองทางกฎหมายมากกว่า เช่น ข้อมูลสุขภาพ ข้อมูลอาชญากรรม ข้อมูลความเชื่อทางศาสนาหรือปรัชญา เป็นต้น โดยจะต้องพิจารณาฐานทางกฎหมายนอกเหนือไปจากฐานทางกฎหมายในกรณีธรรมดา (มาตรา 26) ประกอบด้วย เมื่อได้ดำเนินการขั้นตอนนี้เรียบร้อยแล้วลำดับต่อไปจึงไปพิจารณาว่าเราจะดำเนินการกับข้อมูลอย่างไรบ้างและมีหน้าที่ความรับผิดชอบเกี่ยวกับการประมวลผลข้อมูลเหล่านั้นอย่างไรต่อไป

หน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลนั้นมีหลายประการ ที่พอจะสรุปได้สั้น ๆ ได้แก่ หน้าที่เก็บบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (record of processing activities) หน้าที่แจ้งเจ้าของข้อมูลเมื่อมีการเก็บรวบรวมข้อมูล (information to be provided to data subjects) การบริหารจัดการและปฏิบัติตามสิทธิของเจ้าของข้อมูลเมื่อเจ้าของข้อมูลร้องขอ การมีมาตรการในการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่เหมาะสม การตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดทำการประเมินผลกระทบในการคุ้มครองข้อมูลส่วนบุคคล (data protection impact assessment: DPIA) การควบคุมให้การโอนข้อมูลไปยังต่างประเทศเป็นในโดยชอบด้วยกฎหมาย (cross-border transfer of personal data) เป็นต้น หน้าที่เหล่านี้ในบางอย่างมีการปฏิบัติกันในองค์กรอยู่แล้ว แต่บางอย่างยังไม่มี ในส่วนนี้จึงต้องมีการทบทวนการปฏิบัติในองค์กรเพื่อปรับปรุงสิ่งที่มีอยู่แล้วให้ดีขึ้น ในส่วนที่ยังไม่มีก็ควรที่จะทำเพิ่มเติมขึ้น กระบวนการนี้บางทีก็เรียกว่าการวิเคราะห์หาช่องว่างหรือจุดอ่อน (gap analysis) เพื่ออุดช่องว่างเหล่านั้น

คณะกรรมาธิการยุโรป (European Commission) ได้รวบรวมสถิติใน 1 ปีแรกนับจากที่ GDPR ใช้บังคับเกี่ยวกับการร้องเรียน (complaints) ว่ากิจกรรมที่ได้รับการร้องเรียนมากที่สุด 3 อันดับ ได้แก่ การทำการตลาดผ่านทางโทรศัพท์ (telemarketing) การส่งอีเมลเสนอโปรโมชันสินค้าบริการ (promotional emails) และการติดกล้องวงจรปิด (video surveillance & CCTV)[11] โดยประเด็นที่มีการลงโทษปรับนั้นส่วนใหญ่จะเป็นประเด็นการประมวลผลไม่มีฐานทางกฎหมายรองรับ (ถ้าเทียบกับกฎหมายไทยคือมาตรา 24 และมาตรา 27) และประเด็นการขาดมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคล (security of processing) (ถ้าเทียบกับกฎหมายไทยคือมาตรา 37 ในกรณีของผู้ควบคุมข้อมูลส่วนบุคคล และมาตรา 40 ในกรณีของผู้ประมวลผลข้อมูลส่วนบุคคล)[12] ดังนั้นใน 2 ประเด็นข้างต้นน่าจะเป็นประเด็นที่เราจะต้องให้ความสำคัญเป็นพิเศษในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

---

[11] European Commission, "GDPR in numbers," (2019) accessed 11 Feb 2020, from https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.

[12] โปรดดูเว็บไซต์ที่พยายามเก็บรวบรวมข้อมูลเกี่ยวกับการปรับของผู้กำกับดูแลในกลุ่มประเทศสหภาพยุโรป เช่น https://www.privacyaffairs.com/gdpr-fines/ หรือ https://www.enforcementtracker.com/ เป็นต้น.

ข้อความส่งท้าย

ตามที่ได้กล่าวไปข้างต้นว่ากฎหมายฉบับนี้ยังมีคำถามที่รอคำตอบอยู่หลายประการ และหลายประเด็นน่าจะก่อให้เกิดปัญหาในทางปฏิบัติได้ไม่น้อยเลยทีเดียว คนสำคัญที่น่าจะให้คำตอบได้ในหลายข้อคือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่จะมีขึ้นอนาคตซึ่งจะมีส่วนสำคัญอย่างยิ่งที่จะยกระดับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยให้สูงขึ้น ในขณะเดียวกันก็ต้องกำกับดูแลและบังคับใช้กฎหมายให้สอดคล้องกับการปรับตัวในภาคธุรกิจให้ภาคธุรกิจสามารถเดินไปได้เช่นเดียวกัน