วันที่ 30 มกราคม 2562

นางเสาวณี สุวรรณชีพ
ประธานคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....
รัฐสภา
ถนนอู่ทองใน เขตดุสิต
กรุงเทพมหานคร 10300
ประเทศไทย

ความเห็นของบีเอสเอเรื่องร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านประธานคณะกรรมาธิการวิสามัญฯ

ตามที่ข้าพเจ้าได้มีหนังสือลงวันที่ 11 มกราคม 2562 เรื่อง "*ขอพบเพื่อเรียนเสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์*" นั้น ในนามของบีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ ("**บีเอสเอ**")[1] และสมาชิกของบีเอสเอ ข้าพเจ้าขอขอบพระคุณที่สภานิติบัญญัติแห่งชาติได้กรุณาให้โอกาสในการแสดงความเห็นและข้อแนะนำเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

[1] บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชั่นซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. และมีการดำเนินการในกว่า 60 ประเทศทั่วโลก โดยเป็นผู้ริเริ่มโครงการส่งเสริมการปฏิบัติตามกฎหมายเพื่อรณรงค์การใช้ซอฟต์แวร์ที่ถูกกฎหมาย และสนับสนุนนโยบายสาธารณะที่ส่งเสริมให้มีการสร้างสรรค์นวัตกรรมเทคโนโลยีและขับเคลื่อนให้เศรษฐกิจดิจิทัลเติบโต

สมาชิกของบีเอสเอรวมถึงบริษัท Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio และ Workday

บีเอสเอขอแสดงความชื่นชมต่อรัฐบาลไทย สภานิติบัญญัติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีกรอบกฎหมายที่เข้มแข็งเพื่อคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว ตลอดจนจัดการและระงับยับยั้งภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ กรอบกฎหมายที่มีประสิทธิภาพสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลที่มีความยืดหยุ่นอย่างเหมาะสมจะช่วยเสริมสร้างความเชื่อมั่นซึ่งเป็นสิ่งจำเป็นในการกระตุ้นให้ทุกภาคส่วนมีส่วนร่วมอย่างเต็มที่ในการขับเคลื่อนเศรษฐกิจดิจิทัล อีกทั้งสร้างสรรค์นวัตกรรมบริการและเทคโนโลยีต่างๆ ที่จะช่วยผลักดันให้บรรลุตามเป้าหมายและความเร่งด่วนของ Thailand 4.0 ได้โดยตรง

ก่อนหน้านี้ ข้าพเจ้าได้มีหนังสือถึงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและคณะกรรมการกฤษฎีกาเพื่อแสดงความกังวลและเสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งข้าพเจ้าได้แนบสำเนาไปพร้อมกับหนังสือของข้าพเจ้าถึงสภานิติบัญญัติแห่งชาติ ฉบับวันที่ 11 มกราคม 2562 แล้ว โดยหนังสือดังกล่าวสามารถเข้าถึงทางออนไลน์ได้ที่ลิงค์ต่อไปนี้

- ความเห็นของบีเอสเอเรื่องร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (30 พฤศจิกายน 2561)[2]
- ความเห็นของบีเอสเอเรื่องร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (12 ตุลาคม 2561)[3]
- ความเห็นเพิ่มเติมของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (21 พฤษภาคม 2561)[4]
- ความเห็นของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (17 เมษายน 2561)[5] และ
- ความเห็นของบีเอสเอเรื่องร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (6 พฤษภาคม 2558)[6]

ความเห็นที่แสดงไว้ในหนังสือข้างต้นนี้สามารถนำมาปรับใช้ได้กับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับปัจจุบันเช่นกัน อย่างไรก็ดี ข้าพเจ้าขอเรียนย้ำต่อสภานิติบัญญัติแห่งชาติถึงประเด็นสำคัญที่บีเอสเอและสมาชิกยังคงมีความกังวลดังต่อไปนี้

1. **กรอบกฎหมายในเรื่องกระบวนการที่ชอบด้วยกฎหมายและการอุทธรณ์สามารถปรับให้มีประสิทธิภาพยิ่งกว่านี้ได้** การกำหนดให้หน่วยงานเอกชนมีหน้าที่ใดๆ และการให้อำนาจในการตรวจสอบแก่หน่วยงานของรัฐ (หรือหน่วยงานอื่นใด) ต้องได้รับคำสั่งหรือหมายศาลที่ชอบด้วยกฎหมาย

[2] https://www.bsa.org/~/media/Files/Policy/Data/en11302018BSACommentsCybersecurityBill15November2018.pdf

[3] https://www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

[4] https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf

[5] https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf

[6] https://www.bsa.org/~/media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf

และมีผลผูกพัน โดยหน่วยงานเอกชนต้องมีสิทธิอุทธรณ์หรือโต้แย้งคำสั่งหรือหมายศาลนั้นได้ นอกจากนี้ คำสั่งหรือหมายศาลนั้นจะใช้บังคับได้เฉพาะกับบริษัทที่เป็นผู้ดำเนินการหรือควบคุมโครงสร้างพื้นฐานสำคัญในประเทศไทยเท่านั้น การกำหนดหน้าที่ใดๆ ให้กับหน่วยงานเอกชน และการให้อำนาจใดๆ แก่หน่วยงานของรัฐ (หรือหน่วยงานอื่นใด) ต้องมีความชัดเจน สามารถอุทธรณ์ได้ และได้สัดส่วนตามเจตนารมณ์ของกฎหมาย ดังนั้น การกำหนดให้ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์มีบทบัญญัติในเรื่องต่อไปนี้จึงจะก่อให้เกิดประโยชน์เป็นอย่างยิ่ง

เอ. กำหนดให้ศาลมีอำนาจในการออกคำสั่งต่อบริษัทที่เป็นผู้ดำเนินการจัดการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ไม่ว่าเป็นบริษัทของภาครัฐหรือเอกชน) ไม่ใช่ต่อผู้ให้บริการ

บี. สิทธิในการอุทธรณ์คำสั่งควรครอบคลุมถึงภัยคุกคามทางไซเบอร์ทั้งหมด ไม่ว่าจะมีระดับความรุนแรงเพียงใดก็ตาม

ซี. ควรมีหน่วยงานอิสระที่ทำหน้าที่ในการกำกับดูแลการใช้อำนาจของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“**กปช.**”)

นอกจากนี้ บทบัญญัติใดๆ ที่บัญญัติไว้อย่างกว้างและครอบคลุมทุกกรณี (เช่น มาตรา 66) ซึ่งให้อำนาจอย่างไม่จำกัดแก่หน่วยงานของรัฐหรือหน่วยงานอื่นนั้นควรตัดออก อำนาจ หน้าที่ หรือสิทธิใดๆ ตามร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ควรจะกำหนดไว้อย่างชัดเจน และควรมีการตรวจสอบและถ่วงดุลอย่างเหมาะสม อีกทั้งได้สัดส่วนตามเจตนารมณ์ของกฎหมาย

2. **การรับรอง มาตรฐาน หรือประมวลจริยธรรมที่จัดทำขึ้นต้องสอดคล้องกับวิธีปฏิบัติที่ดีและมาตรฐานอุตสาหกรรมที่สากลยอมรับ** ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ได้กล่าวถึงแนวทาง ประมวลจริยธรรม แนวปฏิบัติ กรอบมาตรฐาน และเอกสารอื่นๆ ที่จัดทำขึ้นเพื่อใช้เป็นแนวทาง (เช่น ถ้อยคำในมาตรา 53 ในร่างพระราชบัญญัติฯ ฉบับปัจจุบัน ซึ่งเรียกรวมกันว่า “กรอบมาตรฐาน”) การที่กรอบมาตรฐานและวิธีปฏิบัติที่ดีจะใช้งานได้อย่างมีประสิทธิภาพสูงสุดนั้นควรต้องจัดทำขึ้นโดยความร่วมมือกับภาคเอกชน โดยที่ภาคเอกชนนำกรอบมาตรฐานและวิธีปฏิบัติที่ดีเหล่านั้นไปใช้เองด้วยความสมัครใจ และควรต้องเป็นกรอบมาตรฐานและวิธีปฏิบัติที่ดีที่เป็นที่ยอมรับในทั่วโลก วิธีปฏิบัติและกรอบมาตรฐานใดๆ ที่ประเทศไทยจะได้จัดทำขึ้นควรเป็นไปในแนวทางเดียวกันกับวิธีจัดการความเสี่ยงที่ใช้อยู่ในอุตสาหกรรม ซึ่งรวมถึงมาตรฐานในกลุ่ม ISO/IEC 27000 หรือกรอบมาตรฐานสำหรับโครงสร้างพื้นฐานสำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ [แห่งสหรัฐอเมริกา] (**NIST**)[7]

3. **ประเภทของข้อมูลที่ได้รับการยกเว้นไม่ต้องถูกเปิดเผย** ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ควรกำหนดประเภทของข้อมูลที่ได้รับการยกเว้นไม่ต้องถูกเปิดเผย เช่น ข้อมูลอันเป็น

[7] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

ความลับหรือข้อมูลที่อาจละเมิดสิทธิอื่นๆ เช่น ข้อมูลส่วนบุคคล หรือข้อมูลที่หากเปิดเผยจะเป็นการขัดกับการปกป้องสิทธิในทรัพย์สินทางปัญญาหรือความลับทางการค้า

4. **ความหมายของ “โครงสร้างพื้นฐานสำคัญ” และ “ภัยคุกคามทางไซเบอร์” ควรสอดคล้องกับวิธีปฏิบัติของสากล** ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับปัจจุบันได้ให้คำนิยามของ “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” และ “ภัยคุกคามทางไซเบอร์” ไว้ อย่างไรก็ดี ข้าพเจ้าขอเรียนเสนอว่าคำนิยามเหล่านี้ในร่างพระราชบัญญัติฯ ควรสอดคล้องกับวิธีปฏิบัติของสากล โดยให้ความหมายหรือคำจำกัดความไว้ดังนี้

   เอ. โครงสร้างพื้นฐานที่สำคัญ “ทรัพย์สิน บริการ และระบบ ไม่ว่าที่จับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารถใช้การได้เป็นระยะเวลานานแล้ว จะส่งผลกระทบในวงกว้างต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ” ทั้งนี้ ในการกำหนดว่าโครงสร้างพื้นฐานใดเป็นโครงสร้างพื้นฐานที่สำคัญนั้น กปช. ควรพิจารณาจากความสำคัญ ความจำเป็นต่อระบบอื่น และระดับความเสี่ยง

   บี. “หน่วยงาน” โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ควรหมายถึงเฉพาะหน่วยงานที่มีอำนาจในการควบคุมโครงสร้างพื้นฐานที่สำคัญได้จริง หรือมีความรับผิดชอบในโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น โดยในทางกฎหมายแล้วหน่วยงานเหล่านี้จะเป็นเจ้าของทรัพย์สินที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ควรระบุไว้อย่างชัดเจนว่า “เครื่องคอมพิวเตอร์” และ “ระบบคอมพิวเตอร์” ที่ไม่มีส่วนใดส่วนหนึ่งอยู่ในประเทศไทยจะไม่ถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตัวอย่างเช่น องค์กรระหว่างประเทศที่มีสำนักงานในประเทศไทยอาจได้รับการสนับสนุนทางโครงสร้างพื้นฐานและระบบเทคโนโลยีสารสนเทศที่ไม่มีส่วนใดส่วนหนึ่งอยู่ในประเทศไทยเลย การกำหนดให้เครื่องคอมพิวเตอร์และระบบคอมพิวเตอร์ดังกล่าวเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจเป็นการขัดแย้งกับแผนการกำกับดูแลของประเทศอื่นได้

   ซี. ภัยคุกคามทางไซเบอร์ที่อยู่ในระดับร้ายแรง หมายความว่า “เหตุภัยคุกคามทางไซเบอร์ที่ทำให้

   - มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีการถูกปฏิเสธไม่ให้เข้าถึงข้อมูล หรือมีการทำลาย ลบ ปรับเปลี่ยน หรือระงับข้อมูลที่จำเป็นต่อการทำงานของโครงสร้างพื้นฐานที่สำคัญ หรือ
   - การควบคุมการปฏิบัติการหรือการควบคุมทางเทคนิคที่จำเป็นต่อความปลอดภัยหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญถูกโจมตี”

5. **ช่วงเปลี่ยนผ่านระหว่างวันที่ตรากฎหมายขึ้นกับวันที่มีผลบังคับใช้ควรห่างกันอย่างน้อยสองปี** นอกจากนี้ กฎหมายฉบับนี้ไม่ควรมีผลย้อนหลัง

6. นอกเหนือจากประเด็นข้างต้นแล้ว ข้าพเจ้าขอเรียนเสนอว่า ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ควรใช้บังคับเฉพาะกับองค์กรและผู้ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่**ดำเนินการหรือควบคุมโครงสร้างพื้นฐานสำคัญที่อยู่ในประเทศไทย**เท่านั้น

สำหรับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล บีเอสเอได้มีหนังสือถึงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและคณะกรรมการกฤษฎีกาเพื่อแสดงความกังวลและเสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับก่อนๆ ซึ่งข้าพเจ้าได้แนบสำเนาไปพร้อมกับหนังสือของข้าพเจ้าถึงสภานิติบัญญัติแห่งชาติ ฉบับวันที่ 11 มกราคม 2562 แล้วเช่นกัน หนังสือดังกล่าวสามารถเข้าถึงทางออนไลน์ได้ที่ลิงค์ต่อไปนี้

- ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (6 กุมภาพันธ์ 2561)[8]
- ความเห็นของบีเอสเอเกี่ยวกับการแก้ไขเพิ่มเติมร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่มีการเสนอเพิ่มเติม (4 สิงหาคม 2560)[9] และ
- ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (23 มีนาคม 2558)[10]

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันมีบทบัญญัติที่ดีขึ้นกว่าร่างฉบับก่อนๆ อันทำให้การคุ้มครองความเป็นส่วนตัวของประชาชนไทยมีความเข้มแข็งขึ้น อย่างไรก็ดี ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ยังคงมีบทบัญญัติในหลายเรื่องที่อาจสร้างภาระเกินควรและอาจสร้างความกำกวมในแง่กฎหมายต่ออุตสาหกรรมเทคโนโลยี ข้าพเจ้าจึงขอเรียนเสนอความเห็นและข้อเสนอแนะสำหรับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับวันที่ 28 ธันวาคม 2561 ซึ่งได้แนบมาพร้อมหนังสือนี้ (**ภาคผนวก**)

เพื่อให้แน่ใจว่าผู้บริโภคและภาคธุรกิจจะสามารถไว้วางใจและได้รับประโยชน์สูงสุดจากนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล เช่น ปัญญาประดิษฐ์และเทคโนโลยีอินเทอร์เน็ตที่เชื่อมต่ออุปกรณ์และเครื่องมือต่างๆ (Internet of Things) ได้ สมาชิกบีเอสเอได้ให้ความสำคัญเป็นอย่างยิ่งในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคและความต้องการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ นอกจากนี้ สมาชิกของบีเอสเอเองเป็นผู้จัดให้เทคโนโลยีที่จำเป็นสำหรับการคุ้มครองความปลอดภัยของสารสนเทศในระบบและเครือข่ายต่างๆ ตลอดจนของบุคคลอีกด้วย

บีเอสเอขอขอบพระคุณที่รัฐบาลไทยได้จัดให้มีกระบวนการแสดงความคิดเห็นอย่างเปิดเผยเพื่อจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ บีเอสเอได้ทำงานอย่างใกล้ชิดกับรัฐบาลในทั่วโลกในเรื่องเกี่ยวกับการพัฒนานโยบายและกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล บีเอสเอจึงขอเรียนว่าการจัดทำ บังคับใช้ และดำเนินการตามระเบียบและข้อกำหนดในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยให้สอดคล้องกับวิธีปฏิบัติที่ดีที่ใช้ในระดับสากลเป็นเรื่องที่สมควรอย่างยิ่ง

---

[8] https://www.bsa.org/~/media/Files/Policy/Data/02062018BSASubmissionThaiPersonalDataProtectionBill.pdf

[9] https://www.bsa.org/~/media/Files/Policy/Data/08042017BSACommentsrePersonalDataProtBill.PDF

[10] https://www.bsa.org/~/media/Files/Policy/Data/03232015BSASubmissiononThaiPersonalDataProtectionAct_EN.PDF

ข้าพเจ้าหวังว่าความเห็นของบีเอสเอจะเป็นประโยชน์ต่อคณะกรรมาธิการฯ และสมาชิกรัฐสภาในการพิจารณาร่างพระราชบัญญัติทั้งสองฉบับนี้เพื่อตราขึ้นเป็นกฎหมายต่อไป

หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อผู้แทนในประเทศไทยของบีเอสเอ นางสาววารุณี รัชต-พัฒนากุล ได้ที่หมายเลข +668-1840-0591 หรือ varuneer@bsa.org

บีเอสเอขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

ดร. เจเร็ด วิลเลียม แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชียแปซิฟิก

ภาคผนวก ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

บีเอสเอขอขอบพระคุณที่รัฐบาลไทยและสภานิติบัญญัติแห่งชาติได้เปิดรับฟังความคิดเห็นเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ทางบีเอสเอได้เฝ้าติดตามการจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างใกล้ชิด และทำงานร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และรู้สึกซาบซึ้งที่การจัดทำร่างพระราชบัญญัติดังกล่าวเป็นไปอย่างโปร่งใส

สมาชิกของบีเอสเอเป็นบริษัทแนวหน้าด้านนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล ซึ่งรวมถึงเทคโนโลยีต่างๆ ที่ใช้คลาวด์คอมพิวติ้ง การวิเคราะห์ข้อมูล ส่วนการเรียนรู้ของเครื่อง (Machine learning) และนวัตกรรมเทคโนโลยีและบริการอื่นๆ ที่ผลักดันการเติบโตของเศรษฐกิจ ด้วยเหตุนี้ สมาชิกของบีเอสเอจึงตระหนักถึงความสำคัญของการเสริมสร้างความไว้เนื้อเชื่อใจและความเชื่อมั่นในบริบทออนไลน์ อันทำให้สมาชิกของบีเอสเอล้วนมีความมุ่งมั่นที่จะคุ้มครองข้อมูลส่วนบุคคลผ่านเทคโนโลยีและโมเดลธุรกิจต่างๆ

บีเอสเอและสมาชิกของบีเอสเอเห็นว่าการตรากฎหมายที่มีประสิทธิภาพซึ่งรวมประเด็นต่างๆ ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นก้าวสำคัญที่แสดงถึงความพยายามของประเทศไทยในการใช้เศรษฐกิจดิจิทัลในการผลักดันการเติบโตของเศรษฐกิจและการสร้างงาน การพัฒนาเทคโนโลยีเหล่านี้อย่างต่อเนื่องจำเป็นต้องมีกรอบกฎหมายที่มีความชัดเจนและยืดหยุ่นอย่างเหมาะสม อันจะคุ้มครองความเป็นส่วนตัวของผู้บริโภคได้โดยที่ไม่ขัดขวางการรับส่งข้อมูลระหว่างประเทศ ซึ่งเป็นดั่งเส้นเลือดที่หล่อเลี้ยงเศรษฐกิจในศตวรรษที่ 21

บีเอสเอได้เรียนเสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับเดือนกุมภาพันธ์ 2561 โดยมีความมุ่งหมายที่จะบรรลุวัตถุประสงค์เหล่านี้ ซึ่งร่างพระราชบัญญัติฉบับปัจจุบันนี้มีบทบัญญัติที่ดีขึ้นกว่าฉบับก่อนๆ อันจะทำให้การคุ้มครองข้อมูลส่วนบุคคลของประชาชนชาวไทยจะเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ดี ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ยังมีบทบัญญัติหลายเรื่องที่อาจก่อให้เกิดภาระเกินสมควรและสร้างความกำกวมในแง่กฎหมายต่ออุตสาหกรรมเทคโนโลยี ในการเสนอความเห็นในครั้งนี้ มีข้อกังวลและประเด็นสำคัญดังต่อไปนี้

1. ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรกำหนดมาตรฐานความรับผิดของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลไว้อย่างชัดเจน โดยอนุญาตให้สามารถผลักความรับผิดโดยอาศัยสัญญาได้ กล่าวคือ ผู้ควบคุมข้อมูลควรเป็นบุคคลที่มีหน้าที่หลัก ในขณะที่ผู้ประมวลผลข้อมูลเพียงปฏิบัติตามคำสั่งตามสัญญาที่จัดทำขึ้น

2. ควรให้คำจำกัดความของข้อมูลส่วนบุคคลอย่างชัดเจน ข้อมูลติดต่อทางธุรกิจและข้อมูลที่ถูกทำให้ไม่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้โดยมีการใช้มาตรการทางเทคนิคและมาตรการในองค์กรที่มีประสิทธิภาพที่จะลดความเสี่ยงให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้อีกครั้งนั้น ไม่ควรถือเป็นข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

3. การกำหนดหลักการให้ผู้ควบคุมข้อมูลแจ้งข้อมูลและได้รับความยินยอมทำให้เกิดความชัดเจนได้ แต่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ควรมีความยืดหยุ่นโดยให้ผู้ควบคุมข้อมูลตัดสินเองได้ว่าการใช้หลักการเหล่านี้ควรดำเนินการอย่างไรจึงจะเป็นวิธีการที่ดีที่สุด

4. ข้อกำหนดเรื่องการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศไม่ได้ช่วยส่งเสริมให้บรรลุตามเป้าหมายของการคุ้มครองข้อมูลส่วนบุคคล แต่กลับขัดขวางการประกอบธุรกิจและทำให้การจัดให้บริการมีต้นทุนสูงขึ้น ข้อกำหนดเรื่องมาตรฐานที่เพียงพอและเงื่อนไขอื่นๆ ของการโอนข้อมูลไปยังต่างประเทศที่จะกำหนดให้มีนั้นควรมีความสอดคล้องให้มากที่สุดกับกลไกที่มีอยู่ตามกรอบกฎหมายในเรื่องการคุ้มครองข้อมูลของประเทศที่เป็นตลาดสำคัญๆ

5. ข้อกำหนดการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลควรมุ่งเน้นไปที่การช่วยให้เจ้าของข้อมูลพ้นจากความเสียหาย และไม่ควรขัดขวางการดำเนินการของธุรกิจเมื่อเกิดเหตุด้านการรักษาความมั่นคงปลอดภัย นอกจากนี้ กฎหมายควรมีกลไกที่ช่วยกระตุ้นให้มีการปฏิบัติตาม เช่น กำหนดให้มีข้อยกเว้นของหน้าที่ในการแจ้งเหตุการละเมิดหากผู้มีหน้าที่รักษาข้อมูลนั้นได้ใช้มาตรการในองค์กรและมาตรการทางเทคนิคที่เพียงพอ (เช่น มีการเข้ารหัสที่ซับซ้อน) เพื่อทำให้ข้อมูลนั้นไม่สามารถนำไปใช้ได้แล้ว

6. เด็กควรได้รับการคุ้มครองในระดับที่สูงขึ้น แต่การกำหนดอายุของบุคคลที่ต้องได้รับการคุ้มครองที่สูงขึ้นไว้ที่ 20 ปี ไม่สอดคล้องกับวิธีการในทั่วโลกที่ใช้เพื่อรักษาความเป็นส่วนตัวของเด็ก การกำหนดอายุของเด็กเพื่อวัตถุประสงค์ในการให้การคุ้มครองในระดับสูงขึ้นไว้ที่ 13 ปี จะสามารถให้การคุ้มครองที่เพียงพอสำหรับเด็กวัยเยาว์ซึ่งมีความเปราะบางเป็นพิเศษได้ ในขณะที่ทำให้ผู้เยาว์ที่โตกว่าได้รับประโยชน์จากบริการที่เกี่ยวข้องกับข้อมูลได้อย่างง่ายดายด้วย

7. การบัญญัติสิทธิของผู้บริโภค เช่น สิทธิในการขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนและสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตน เป็นการเพิ่มการคุ้มครองให้แก่ผู้บริโภคได้ อย่างไรก็ดี การที่จะทำให้การใช้สิทธิเหล่านี้สามารถกระทำได้ในทางปฏิบัติ ควรต้องมีการปรึกษาหารืออย่างใกล้ชิดกับภาคเอกชนในการจัดทำแนวทาง ประกาศ และกฎหมายลำดับรอง

8. หลักเกณฑ์ที่ทำให้มีความจำเป็นต้องจัดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับอื่นๆ และใช้กับผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลที่กระทำกิจกรรมหลักเกี่ยวกับการตรวจสอบในเชิงระบบเป็นประจำของเจ้าของข้อมูลจำนวนมากเท่านั้น นอกจากนี้ ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรกำหนดให้ชัดเจนว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่จำเป็นต้องอยู่ในประเทศไทย และเครือกิจการเดียวกันสามารถแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขึ้นเพียงรายเดียวก็ได้

9. การที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (**คณะกรรมการ**) และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (**สำนักงาน**) กระทำการในลักษณะที่ยุติธรรม โปร่งใส และเป็นมาตรฐานเป็นเรื่องที่สำคัญยิ่ง อีกทั้งอำนาจของคณะกรรมการและสำนักงานควรจำกัดอย่างเหมาะสม โดยเฉพาะในส่วนที่เกี่ยวข้องกับการใช้ร่างพระราชบัญญัตินี้และการดำเนินการตรวจสอบ

10. โทษและทางแก้ไขเยียวยาที่มีประสิทธิภาพเป็นองค์ประกอบสำคัญของกรอบกฎหมายการคุ้มครองข้อมูลส่วนบุคคล แต่การกำหนดให้มีโทษทางอาญาและความรับผิดเป็นการส่วนตัวไม่ได้สัดส่วนกับความเสี่ยงที่จะเกิดความเสียหายในบริบทของกฎหมายนี้ ไม่สอดคล้องกับวิธีปฏิบัติที่ดีที่สากลยอมรับ อีกทั้งอาจระงับการดำเนินการประมวลผลข้อมูลที่เป็นไปโดยชอบด้วยกฎหมายได้
11. ขอบเขตการบังคับใช้ร่างพระราชบัญญัติฯ ควรจำกัดอยู่ที่นิติบุคคลหรือกิจกรรมที่มีความเกี่ยวข้องใกล้ชิดอย่างเพียงพอกับประเทศไทยเพื่อให้แน่ใจว่าจะสามารถบังคับสิทธิได้อย่างมีประสิทธิภาพ
12. ระยะเวลาที่เหมาะสมระหว่างวันที่ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกับวันที่มีผลบังคับใช้ควรห่างกันไม่น้อยกว่าสองปีเพื่อให้มีช่วงเปลี่ยนผ่านที่ราบรื่นทั้งต่อบุคคล ธุรกิจ และหน่วยงานของรัฐ

บีเอสเอขอเรียนอธิบายความเห็นและข้อเสนอแนะโดยละเอียดเพื่อให้ท่านพิจารณาดังต่อไปนี้

การแยกความแตกต่างอย่างชัดเจนระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล (มาตรา 37, 39, 75-76 และ 83-86)

ในเบื้องต้น บีเอสเอได้เน้นถึงประเด็นสำคัญเกี่ยวกับการให้คำจำกัดความที่บีเอสเอยังคงมีความกังวลอย่างยิ่ง นั่นก็คือ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ยังคงมีความไม่ชัดเจนระหว่าง “ผู้ควบคุมข้อมูลส่วนบุคคล” (**ผู้ควบคุมข้อมูล**) กับ “ผู้ประมวลผลข้อมูลส่วนบุคคล” (**ผู้ประมวลผลข้อมูล**) การแบ่งความรับผิดชอบและความรับผิดระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลนั้นเป็นเรื่องจำเป็นเพื่อให้แน่ใจว่าการจัดจ้างบุคคลภายนอกให้ทำงานให้ (Outsourcing) ซึ่งเป็นการปฏิบัติที่แพร่หลายนั้นจะไม่ก่อให้เกิดความสับสนในภาพรวมของการคุ้มครองข้อมูลส่วนบุคคล

บุคคลที่มีความสัมพันธ์โดยตรงกับเจ้าของข้อมูลส่วนบุคคล (**เจ้าของข้อมูล**) ได้แก่ผู้ควบคุมข้อมูล ไม่ใช่ผู้ประมวลผลข้อมูล โดยผู้ประมวลผลข้อมูลเป็นผู้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล อันเป็นหน้าที่ตามสัญญาระหว่างผู้ประมวลผลข้อมูลกับผู้ควบคุมข้อมูล ด้วยเหตุนี้ ผู้ควบคุมข้อมูลจึงควรเป็นบุคคลหลักที่มีความรับผิดชอบและหน้าที่ในการดำเนินการให้แน่ใจว่ามีการปฏิบัติตามกฎหมายและข้อกำหนดที่ใช้บังคับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลควรมีหน้าที่เพียงปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลและดูแลให้ข้อมูลส่วนบุคคลที่ตนประมวลผลในนามของผู้ควบคุมข้อมูลนั้นมีความมั่นคงปลอดภัย ความสัมพันธ์ระหว่างผู้ประมวลผลข้อมูลกับผู้ควบคุมข้อมูลควรเป็นไปตามสัญญา

การกำหนดให้ผู้ประมวลผลข้อมูลมีความรับผิดโดยตรง ความรับผิดร่วมกันหรือแยกกัน หรือความรับผิดอื่นๆ อาจก่อให้เกิดผลที่ไม่ประสงค์ให้เกิดขึ้นได้หลายประการ อีกทั้งเป็นการบั่นทอนความสัมพันธ์ระหว่างผู้ประมวลผลข้อมูลกับผู้ควบคุมข้อมูล และทำให้เกิดปัญหาเกี่ยวกับการปฏิบัติตามกฎหมายและการบังคับสิทธิที่ไม่ควรต้องเกิดขึ้น นอกจากนี้ยังอาจส่งผลต่อการลงทุนและนวัตกรรมเกี่ยวกับการประมวลผลข้อมูล และการจัดจ้างบุคคลภายนอก (Outsourcing) อีกด้วย

ข้อเสนอแนะ

เพื่อแบ่งแยกหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอย่างชัดเจน บีเอสเอขอเรียนเสนอให้มีการแก้ไขเพิ่มเติมดังนี้

- แก้ไขเพิ่มเติมเกี่ยวกับ “หน้าที่” ของผู้ประมวลผลข้อมูลใน**มาตรา 39** เพื่อให้เกิดความชัดเจนในเรื่องความรับผิดของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- ตัดข้อกำหนดในส่วนของ “ผู้ประมวลผลข้อมูล” ที่ควรเป็นข้อกำหนดสำหรับ “ผู้ควบคุมข้อมูล” ตลอดทั้งร่างพระราชบัญญัติฯ ออก

ข้อเสนอแนะข้างต้นนี้เป็นไปตามเหตุผลดังต่อไปนี้

I. การแก้ไขเพิ่มเติมในมาตรา 39 ที่เรียนเสนอ

มาตรา 39 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก่อให้เกิดความสับสนเกี่ยวกับบทบาทหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล อีกทั้งทำให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลมีความรับผิดร่วมกัน โดยการบัญญัติว่า

> *“...ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลนั้น”*

นอกจากนี้ ถ้อยคำในร่างพระราชบัญญัติฯ ฉบับปัจจุบันนี้ขัดแย้งอย่างเห็นได้ชัดกับคำจำกัดความของผู้ประมวลผลข้อมูลใน**มาตรา 6** ซึ่งบัญญัติไว้ว่า “*... ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล”*

บีเอสเอขอเรียนเสนอว่า**มาตรา 39** ควรแก้ไขเพิ่มเติมดังนี้

(เอ) **<u>ตัดข้อความส่วนหลังของอนุมาตรา (1) ออก</u>** เนื่องจากผู้ประมวลผลข้อมูลอาจไม่ทราบถึงลักษณะของข้อมูลที่จัดให้แก่ตน การให้ความยินยอมโดยเจ้าของข้อมูลหรือการติดต่อสื่อสารกับเจ้าของข้อมูลที่ผู้ควบคุมข้อมูลจัดให้มีขึ้น หรือข้อกำหนดโดยเฉพาะเจาะจงตามกฎหมายที่เกี่ยวข้องกับข้อมูลนั้น ผู้ควบคุมข้อมูลควรรับผิดชอบในการดำเนินการให้มั่นใจได้ว่าคำสั่งที่ตนมีต่อผู้ประมวลผลข้อมูลไม่ขัดต่อหน้าที่ใดๆ ที่มีตามกฎหมาย การกำหนดให้ผู้ประมวลผลข้อมูลมีหน้าที่ในการตรวจสอบและยืนยันว่าคำสั่งของผู้ควบคุมข้อมูลเป็นคำสั่งที่ชอบด้วยกฎหมายเป็นข้อกำหนดที่ไม่สมเหตุสมผลและไม่สามารถนำไปปฏิบัติได้จริง เช่น โดยทั่วไปแล้วเมื่อผู้ควบคุมข้อมูลสั่งให้ผู้ประมวลผลข้อมูลประมวลผลข้อมูลที่ผู้ควบคุมข้อมูลได้เก็บรวบรวม ผู้ประมวลผลข้อมูลจะไม่สามารถตรวจสอบเองได้เลยว่าได้มีการขอความยินยอมโดยชอบและแจ้งข้อมูลให้เจ้าของข้อมูลทราบอย่างเพียงพอแล้วหรือไม่

(บี) **<u>แก้ไขเพิ่มเติมอนุมาตรา (2)</u>** เพื่อให้หน้าที่ของผู้ประมวลผลข้อมูลในการรักษาข้อมูลมีความชัดเจน โดยบีเอสเอขอเสนอให้ตัดข้อความต่อไปนี้ออก *“การสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ”* เนื่องจากเป็นการกำหนดหน้าที่เกินจำเป็น นอกจากนี้ อนุมาตรานี้ไม่ควรกำหนดหน้าที่ในการแจ้งเหตุการละเมิดที่นอกเหนือไปจากหน้าที่ในการแจ้งตามมาตรา 36(4) บีเอสเอจึงขอเสนอให้ตัดข้อความ “รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น” ออกด้วย

(ซี) **<u>ตัดอนุมาตรา (3) ออก</u>** เนื่องจากการคาดหวังให้ผู้ประมวลผลข้อมูลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลต่างๆ ที่ตนอาจได้ดำเนินการนั้นเป็นเรื่องที่ไม่สมเหตุสมผล บีเอสเอขอเรียนย้ำอีกครั้งหนึ่งว่า ผู้ประมวลผลข้อมูลอาจมีข้อมูลเพียงเล็กน้อยเกี่ยวกับลักษณะของข้อมูลที่ตนประมวลผลในนามของบุคคลอื่น และในความเป็นจริงแล้วอาจดำเนินการเพื่อให้มั่นใจว่าตนจะทราบถึงข้อมูลดังกล่าวให้ได้น้อยที่สุดเพื่อเป็นการรักษาความเป็นส่วนตัวและความปลอดภัยของผู้บริโภคและลูกค้า และข้อมูลของบุคคลเหล่านี้

(ดี) **<u>ตัดวรรคสองออก</u>** เนื่องจากขัดแย้งและก่อให้เกิดความสับสนกับคำจำกัดความของผู้ประมวลผลข้อมูล ทั้งนี้ ตาม**มาตรา 6** ผู้ประมวลผลข้อมูลไม่เป็นผู้ควบคุมข้อมูล และกระทำการ *"ตามคำสั่งหรือในนามของ"* ผู้ควบคุมข้อมูล

(อี) **<u>เติมข้อความว่า *"โดยในแต่ละกรณี ตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลไว้เป็นหนังสือ"* ไว้ในส่วนท้ายของมาตรา 39</u>** เพื่อให้มีความชัดเจนว่าผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอาจผลักความรับผิดให้แก่กันได้ตามสัญญาที่จัดทำขึ้น

โดยสรุป มาตรา 39 ตามที่เสนอให้แก้ไขเพิ่มเติมปรากฏดังนี้

> ***มาตรา 39*** ***ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้***
>
> *(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น* ***~~เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้~~***
>
> *(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย* ***<u>ตามสมควรที่เหมาะสม</u>*** *เพื่อ* ***<u>รักษาความปลอดภัยของข้อมูล</u>~~ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น~~***
>
> ***~~(3) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลไว้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด~~***
>
> ***~~ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลนั้น~~***
>
> ***<u>โดยในแต่ละกรณี ตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลไว้เป็นหนังสือ</u>***

II. การตัดข้อกำหนดอื่น ๆ เกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล (รวมถึงในมาตรา 83-86)

ตามที่กล่าวไว้ข้างต้น ผู้ประมวลผลข้อมูลไม่ได้มีความสัมพันธ์โดยตรงกับเจ้าของข้อมูล และมักไม่ทราบและไม่มีอำนาจควบคุมข้อมูลที่ตนประมวลผลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ด้วยเหตุนี้ ผู้ประมวลผลข้อมูล

(เช่น ผู้ให้บริการคลาวด์) จึงไม่อาจทราบอย่างแน่ชัดได้ว่าข้อมูลที่ตนกำลังประมวลผลอยู่นั้นเป็นข้อมูลส่วนบุคคล เป็นข้อมูลที่มีความละเอียดอ่อน (ตามมาตรา 26) หรือมีข้อมูล “เป็นจำนวนมาก” (ตามมาตรา 40(2)) หรือไม่ ดังนั้น การกำหนดให้ผู้ประมวลผลข้อมูลมีความรับผิดทางแพ่งจากการที่ผู้ประมวลผลข้อมูลทำการประมวลผลข้อมูลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล โดยที่ไม่ทราบว่าข้อมูลที่ตนประมวลผลนั้นเป็นข้อมูลอะไร จึงเป็นบทบัญญัติที่ไม่ได้สัดส่วน เนื่องจากผู้ประมวลผลข้อมูลไม่อาจกำหนดระดับความระมัดระวัง “ตามควร” สำหรับข้อมูลนั้นได้ ดังนั้น บีเอสเอจึงขอแนะนำให้**ตัดผู้ประมวลผลข้อมูลออกจากมาตรา 75-76 และตัดมาตรา 83-86 ออกไป** เนื่องจากโทษทางแพ่งและทางปกครองใน**หมวด 6 และหมวด 7** ควรจำกัดอยู่เพียงผู้ควบคุมข้อมูลเท่านั้น ไม่ควรกำหนดสำหรับผู้ประมวลผลข้อมูลด้วย

การแก้ไขเพิ่มเติมที่เรียนเสนอในหนังสือฉบับนี้ที่มีขึ้นเพื่อให้เกิดความชัดเจนและเป็นการจำกัดข้อกำหนดต่อผู้ประมวลผลข้อมูลนั้นไม่ได้ครอบคลุมบทบัญญัติในทุกมาตรา หากสภานิติบัญญัติจักได้ทบทวนข้อกำหนดทั้งหมดที่เกี่ยวข้องกับผู้ประมวลผลข้อมูลและหลีกเลี่ยงข้อกำหนดต่อผู้ประมวลผลข้อมูลที่ไม่สมเหตุสมผล ไม่จำเป็น และไม่สามารถปฏิบัติได้จริง ในกรณีที่สมควรให้ผู้ควบคุมข้อมูลมีหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลได้นั้นจะเป็นประโยชน์อย่างยิ่ง ทั้งนี้ เพื่อให้แน่ใจว่ากฎหมายฉบับนี้จะส่งเสริมให้การคุ้มครองข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลเป็นไปอย่างมีประสิทธิภาพ โดยที่ไม่ส่งผลเป็นการจำกัดวิธีการประมวลผลข้อมูลเพื่อประโยชน์ของเจ้าของข้อมูล

การให้คำจำกัดความของข้อมูลส่วนบุคคล (มาตรา 6) และข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (Anonymized data) และข้อมูลที่เป็นการใช้นามสมมุติ (Pseudonymized data) (มาตรา 26 และมาตรา 33)

เอ. ข้อมูลติดต่อทางธุรกิจ และข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้/ข้อมูลที่เป็นการใช้นามสมมุติ ไม่ควรอยู่ในขอบเขตคำจำกัดความของข้อมูลส่วนบุคคล

มาตรา 6 ได้ให้คำจำกัดความของ “ข้อมูลส่วนบุคคล” ไว้อย่างกว้าง โดยครอบคลุมข้อมูลทั้งหมดที่เกี่ยวข้องกับบุคคลหนึ่งๆ อันทำให้สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นได้ ซึ่งในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับที่แก้ไขนี้ บีเอสเอสังเกตเห็นว่า คำจำกัดความของข้อมูลส่วนบุคคลไม่ได้ยกเว้นข้อมูลส่วนบุคคลที่เป็น “*การระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ*” ไว้อีกต่อไป

การโอนข้อมูลติดต่อทางธุรกิจมักเกิดขึ้นในหลายๆ ขั้นตอนทางธุรกิจ และการใช้ข้อมูลเหล่านั้นเพื่อวัตถุประสงค์ในการติดต่อทางธุรกิจเป็นที่ทราบกันโดยปริยายว่าจะเกิดขึ้นหากมีการแลกเปลี่ยนข้อมูลติดต่อทางธุรกิจให้แก่กัน นอกจากนี้ ข้อมูลติดต่อทางธุรกิจนั้นจะเป็นของเจ้าของข้อมูลหรือขององค์กรที่จ้างเจ้าของข้อมูลก็เป็นประเด็นที่ยังไม่ทราบได้แน่ชัด ด้วยเหตุนี้ คำจำกัดความของข้อมูลส่วนบุคคลที่รวมไปถึงข้อมูลติดต่อทางธุรกิจด้วยนั้นจะทำให้กิจกรรมระหว่างธุรกิจกับธุรกิจยุ่งยากขึ้นอย่างมีนัยสำคัญ

ข้อเสนอแนะ

บีเอสเอขอเรียนเสนอให้**นำข้อยกเว้นในเรื่องข้อมูลติดต่อทางธุรกิจกลับเข้ามาไว้ในคำจำกัดความของข้อมูลส่วนบุคคล**ใน**มาตรา 6** ดังนี้

"ข้อมูลส่วนบุคคล หมายความว่า. . . ***<u>แต่ไม่รวมถึงข้อมูลที่ระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน ข้อมูลติดต่อทางธุรกิจ หรือที่อยู่ทางธุรกิจของบุคคลหนึ่ง ๆ หากเป็นการใช้เพื่อติดต่อบุคคลนั้น ๆ เพื่อวัตถุประสงค์ทางธุรกิจเท่านั้น</u>*** *"*

บี. ข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้และข้อมูลที่เป็นการใช้นามสมมุติ

มาตรา 26(5)(ง) และมาตรา 33 มีการกล่าวถึงการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้และการใช้นามสมมุติ แต่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไม่ได้นำเงื่อนไขของกฎหมายในเรื่องนี้ไปใช้กับบทบัญญัติในส่วนอื่นๆ เช่น บทบัญญัติเกี่ยวกับหน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและการประเมินความเสี่ยง ในกรณีที่ได้มีการใช้วิธีการอื่นๆ ที่ทำให้ไม่สามารถเชื่อมโยงข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้ (De-identification) ซึ่งรวมถึงการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้และการใช้นามสมมุติ เพื่อลดผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล

<u>ข้อเสนอแนะ</u>

การจูงใจให้มีการใช้วิธีการที่ทำให้ไม่สามารถเชื่อมโยงข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้เพื่อคุ้มครองข้อมูลส่วนบุคคลจะเป็นประโยชน์ทั้งต่อบุคคลและเศรษฐกิจ ทั้งนี้เนื่องจากการใช้วิธีการเหล่านี้จะช่วยลดผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลและลดความเสี่ยงในเรื่องการรักษาความมั่นคงปลอดภัย ในขณะเดียวกัน การใช้ข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การใช้นามสมมุติ หรือการใช้ข้อมูลที่ถูกทำให้ไม่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้ ในลักษณะที่ไม่ต้องอยู่ภายใต้กรอบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะช่วยส่งเสริมให้มีการใช้ข้อมูลในวิธีที่สร้างสรรค์ขึ้นได้

ด้วยเหตุนี้ บีเอสเอจึงขอเรียนเสนอให้**<u>บัญญัติไว้อย่างชัดเจนในคำจำกัดความของข้อมูลส่วนบุคคลว่าไม่รวมถึงข้อมูลที่ถูกทำให้ไม่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้ ที่มีการใช้มาตรการทางเทคนิคและมาตรการในองค์กรที่มีประสิทธิภาพที่จะลดความเสี่ยงได้ตามสมควรที่จะทำให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลนั้นได้อีกครั้ง</u>** ข้อมูลที่ถูกทำให้ไม่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้ ที่มีการใช้มาตรการควบคุมตามสัญญา มาตรการคุ้มครองความเป็นส่วนตัวและรักษาความมั่นคงปลอดภัย หรือทั้งสองอย่าง อันทำให้ลดความเสี่ยงได้ตามสมควรที่จะทำให้ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้อีกครั้งนั้น ไม่ควรอยู่ในความหมายของข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เว้นแต่บทบัญญัติที่เป็นข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยหรือภาระรับผิดชอบ (Accountability)

นอกจากนี้ บีเอสเอเห็นว่า**<u>ในกรณีที่ได้มีการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ การใช้นามสมมุติ หรือการใช้วิธีการอื่น ๆ ที่ทำให้ไม่สามารถเชื่อมโยงข้อมูลส่วนบุคคลไปยังเจ้าของข้อมูลส่วนบุคคลนั้นได้ เพื่อลดผลกระทบต่อสิทธิของเจ้าของ</u>**

<u>ข้อมูลส่วนบุคคล ร่างพระราชบัญญัตินี้ควรนำเงื่อนไขของกฎหมายนี้ไปใช้กับบทบัญญัติในส่วนอื่น ๆ ด้วย</u> เช่น บทบัญญัติเกี่ยวกับหน้าที่ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและการประเมินความเสี่ยง เพื่อเป็นการกระตุ้นให้มีการใช้วิธีปฏิบัติดังกล่าว

การแจ้งและการให้ความยินยอม และหลักเกณฑ์อื่น ๆ ตามกฎหมายที่ทำให้สามารถจัดการข้อมูลส่วนบุคคลได้ (มาตรา 19-29)

มาตรา 19 ถึงมาตรา 29 ได้กำหนดกรอบสำหรับกรณีที่ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงลักษณะของการจัดการข้อมูลส่วนบุคคลที่ตนจะกระทำและหน้าที่ในการขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล เว้นแต่เป็นกรณีตามที่กฎหมายกำหนดไว้โดยเฉพาะ

เอ. กรณีที่ถือว่าเป็นการให้ความยินยอม หรือเป็นการให้ความยินยอมโดยปริยาย

มาตรฐานสำหรับระดับการให้ความยินยอมที่เหมาะสมนั้นควรพิจารณาตามบริบทไป สำหรับในบริบทที่ไม่ได้สื่อให้เห็นว่าอาจเป็นข้อมูลที่มีความละเอียดอ่อนอย่างยิ่ง การให้ความยินยอมโดยปริยายก็อาจเป็นวิธีการที่เหมาะสม

การกำหนดให้การได้รับความยินยอมโดยชัดแจ้งเป็นหนังสือเท่านั้นที่เป็นหลักเกณฑ์ตามกฎหมายเพียงประการเดียวที่ทำให้สามารถจัดการข้อมูลส่วนบุคคลได้อาจส่งผลให้ (1) การเติบโตและการสร้างสรรค์นวัตกรรมในสภาพเศรษฐกิจดิจิทัลชะลอตัวลง และ (2) ไม่เป็นไปตามความคาดหวังของผู้บริโภคในเรื่องการรักษาความเป็นส่วนตัวจากการทำให้ผู้บริโภคเบื่อหน่ายกับการคลิ๊กเพื่อแสดงการให้ความยินยอม (“Click fatigue”) โดยที่ผู้ใช้งานจะยอมรับข้อกำหนดใดก็ตามที่ปรากฏอยู่ตรงหน้าโดยไม่พิจารณาหรือไม่ได้เข้าใจข้อมูลที่ปรากฏนั้นอย่างถ่องแท้

ในโลกที่เป็นยุคดิจิทัลในปัจจุบัน มีข้อมูลจำนวนมากเกิดขึ้นจากการมีปฏิสัมพันธ์กันระหว่างบุคคลผ่านทางอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ต การให้ความยินยอมโดยชัดแจ้งเป็นวิธีการที่ไม่เหมาะสมหรืออาจไม่สามารถปฏิบัติได้จริงในหลายกรณี โดยเฉพาะในกรณีที่ไม่ได้เป็นเรื่องที่มีความละเอียดอ่อนอย่างยิ่ง ตัวอย่างเช่น บริการคมนาคมขนส่งสาธารณะในอนาคตอาจได้รับผลกระทบหากกฎหมายกำหนดให้แต่ละบุคคลให้ความยินยอมอย่างชัดแจ้งเพื่ออนุญาตให้ทางเข้าที่ใช้ระบบอิเล็กทรอนิกส์สร้างข้อมูลทุกครั้งที่บุคคลนั้นใช้บัตรสำหรับบริการคมนาคมขนส่งสาธารณะนั้น ในกรณีดังกล่าวนี้ การให้ความยินยอมโดยปริยายจึงอาจเป็นวิธีการที่เหมาะสม แต่สำหรับในกรณีอื่นๆ เช่น การจัดการข้อมูลสุขภาพหรือข้อมูลทางการเงินซึ่งมีความละเอียดอ่อน การให้ความยินยอมโดยชัดแจ้งอาจเป็นวิธีการที่เหมาะสม

<u>ข้อเสนอแนะ</u>

บีเอสเอขอเรียนเสนอให้สภานิติบัญญัติพิจารณาบริบทต่างๆ ที่อาจมีการจัดการข้อมูลส่วนบุคคลและจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้มีความยืดหยุ่นเพียงพอให้ผู้ควบคุมข้อมูลสามารถกำหนดระยะเวลา มาตรฐาน และกลไกสำหรับการได้รับความยินยอม โดยใน**มาตรา 19** ควรกล่าวถึงกรณีที่ “ถือว่า” เป็นการให้ความยินยอมหรือเป็นการให้ความยินยอม “โดยปริยาย” ไว้ด้วยดังนี้

มาตรา 19 *ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้~~ก่อนหรือในขณะนั้น~~ เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้*

*การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้**หรือในกรณีที่ถือได้ว่าเป็นการให้ความยินยอมหรือเป็นการให้ความยินยอมโดยปริยาย***

บี. หลักเกณฑ์ตามกฎหมายในการจัดการข้อมูลส่วนบุคคล

บีเอสเอเห็นด้วยกับการกำหนดให้มีข้อยกเว้นในเรื่องประโยชน์โดยชอบด้วยกฎหมายใน**มาตรา 24(6)** ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล บีเอสเอเข้าใจว่าประเด็นนี้ได้นำมาจากเหตุผลเรื่อง “ประโยชน์โดยชอบด้วยกฎหมาย” ของระเบียบทั่วไปแห่งสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (**GDPR**)[11] จึงขอเรียนเสนอให้การบังคับใช้**มาตรา 24(6)** นี้มีระดับความยืดหยุ่นเท่าเทียมกับการบังคับใช้เรื่องประโยชน์โดยชอบด้วยกฎหมายของ GDPR โดยหลักในเรื่องประโยชน์โดยชอบด้วยกฎหมายตาม GDPR ของสหภาพยุโรปนั้น องค์กรต่างๆ สามารถขยายโอกาสทางธุรกิจได้ โดยที่สามารถปฏิบัติตามหน้าที่โดยรวมในเรื่องการคุ้มครองข้อมูลได้ในขณะเดียวกัน

นอกจากนี้ การกำหนดให้มีหลักเกณฑ์อื่นๆ ตามกฎหมายในการจัดการข้อมูลส่วนบุคคลที่นอกเหนือจากการได้รับความยินยอม น่าจะเป็นเรื่องที่เหมาะสมยิ่งกว่าการกำหนดให้ประโยชน์โดยชอบด้วยกฎหมายและหลักเกณฑ์อื่นๆ เป็นเพียง “ข้อยกเว้น” ของกรณีที่ต้องได้รับความยินยอม

ข้อเสนอแนะ

บีเอสเอขอเรียนเสนอให้แก้ไขเพิ่มเติมร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้มีการกำหนดถึงหลักเกณฑ์อื่นๆ ในการประมวลผลข้อมูลส่วนบุคคล ที่เพิ่มเติมไปจากการได้รับความยินยอม ไม่ใช่กำหนดไว้เป็นข้อยกเว้นของกรณีที่ต้องได้รับความยินยอม หลักเกณฑ์อื่นๆ นั้นรวมถึงประโยชน์โดยชอบด้วยกฎหมายของบริษัทผู้จัดการข้อมูล การปฏิบัติหน้าที่ตามสัญญาที่มีกับตัวเจ้าของข้อมูลเอง และการปฏิบัติหน้าที่ตามกฎหมาย อนึ่ง กรอบกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้จำเป็นต้องระบุหลักเกณฑ์เพียงประการใดประการหนึ่งในการประมวลผลข้อมูล แต่ควรกำหนดหลักเกณฑ์ตามกฎหมายที่สามารถใช้ได้เป็นการทั่วไป และควรเป็นเรื่องที่ผู้ควบคุมข้อมูลสามารถระบุเหตุผลที่เกี่ยวข้องได้เอง และดำเนินการให้แน่ใจว่าการประมวลผลข้อมูลที่ตนกระทำนั้นเป็นไปตามเหตุผลดังกล่าว

ซี. แบบในการแจ้งและให้ความยินยอม

[11] ระเบียบ (EU) ที่ 2016/679 แห่งรัฐสภายุโรปและคณะมนตรียุโรป ลงวันที่ 27 เมษายน 2559 เรื่อง การคุ้มครองบุคคลธรรมดาในเรื่องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและการโอนข้อมูลนั้นได้อย่างอิสระ และคำสั่งที่ 95/46/EC ที่ใช้แทน

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลยังคงบัญญัติไว้ใน**มาตรา 19** ว่า คณะกรรมการ "*จะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้*"

ในกรณีที่อาจจำเป็นต้องได้รับความยินยอมโดยชัดแจ้ง การจัดทำแนวทางที่ช่วยแนะผู้ควบคุมข้อมูลเกี่ยวกับข้อความที่ควรระบุไว้ในหนังสือขอความยินยอมจากเจ้าของข้อมูลก็อาจเป็นประโยชน์ แต่การกำหนดให้แบบสำหรับการขอและได้รับความยินยอมมีความยืดหยุ่นก็เป็นเรื่องจำเป็นเช่นกัน

เนื่องจากเทคโนโลยีมีการพัฒนาอยู่ตลอดเวลาและมีวิธีการใหม่ๆ มากมายในการใช้ข้อมูลส่วนบุคคลให้เกิดประโยชน์ต่อสังคมและเศรษฐกิจ ในปัจจุบัน ผู้ควบคุมข้อมูลมากมายจึงได้พัฒนากลไกสำหรับการขอและได้รับความยินยอมโดยพิจารณาจากปัจจัยในหลายด้าน แบบสำหรับการขอความยินยอมที่กำหนดไว้ล่วงหน้าอาจล้าสมัยได้ในเวลาอันรวดเร็วและกลับส่งผลให้การพัฒนาอันก่อให้เกิดประโยชน์ดังกล่าวล่าช้าไปได้

ข้อเสนอแนะ

บีเอสเอขอเรียนเสนอให้ตัดข้อความในมาตรา 19 ในส่วนที่เกี่ยวกับแบบสำหรับการขอความยินยอมออกไปดังนี้

> ***มาตรา 19***
>
> *. . .*
>
> *ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องชัดเจน และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว* ~~***ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้***~~

ดี. การแจ้งระยะเวลาในการเก็บรวบรวมข้อมูล

ในเรื่องการแจ้งข้อมูลต่อเจ้าของข้อมูลส่วนบุคคล ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีข้อกำหนดใหม่ใน**มาตรา 23(2)** ซึ่งกำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึง "*ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้*" ซึ่งในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน "*ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม*"

เนื่องด้วยวิธีการเก็บข้อมูลมีลักษณะซ้ำเดิม ในขณะที่มีวิธีใหม่ๆ ในการใช้ข้อมูลส่วนบุคคลเกิดขึ้นอยู่เสมอดังที่ได้เรียนไว้ข้างต้น การกำหนดให้ผู้ควบคุมข้อมูลระบุไว้แต่แรกในขณะเก็บรวบรวมข้อมูลถึงระยะเวลาในการเก็บรวบรวมข้อมูลอาจเป็นเรื่องที่ไม่สามารถทำได้ในทางปฏิบัติได้เสมอไป นอกจากนี้ มาตรา 23(2) ในร่างพระราชบัญญัติฉบับปัจจุบันมีความไม่ชัดเจนว่าผู้ควบคุมข้อมูลจะสามารถกำหนด "*ระยะเวลาที่อาจคาดหมายได้สำหรับการเก็บรวบรวม*" และจะมีการประเมิน "*มาตรฐานของการเก็บรวบรวม*" เพื่อกำหนดระยะเวลาที่คาดหมายสำหรับการเก็บรวบรวมข้อมูลได้อย่างไร

ข้อเสนอแนะ

เนื่องจากในบางกรณี ผู้ควบคุมข้อมูลอาจไม่สามารถกำหนดระยะเวลาสำหรับการเก็บรวบรวมข้อมูลได้ ไม่ว่าตามจริงหรือตามที่ “คาดหมาย” ด้วยเหตุนี้ มาตรา 23(2) จึงควรแก้ไขให้มีความยืดหยุ่นยิ่งขึ้น กล่าวคือ ควรกำหนดให้ผู้ควบคุมข้อมูลแจ้งหลักเกณฑ์และหลักการของนโยบายเกี่ยวกับการเก็บข้อมูลของตน ซึ่งจะเหมาะสมกว่าการกำหนดให้ผู้ควบคุมข้อมูลแจ้งถึงระยะเวลา “ที่อาจคาดหมายได้” ตัวอย่างเช่น ผู้ควบคุมข้อมูลอาจระบุไว้ในนโยบายเกี่ยวกับการเก็บข้อมูลว่า “ข้อมูลส่วนบุคคลจะมีการเก็บไว้ไม่เกินหกเดือนหลังจากวัตถุประสงค์ตามกฎหมายหรือวัตถุประสงค์ทางธุรกิจในการเก็บข้อมูลนั้นไว้ได้สิ้นสุดลง” บีเอสเอขอเรียนเสนอให้แก้ไขมาตรา 23(2) ดังนี้

มาตรา 23(2)

. . .

ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ***<u>ให้ผู้ควบคุมข้อมูลแจ้งข้อมูลเกี่ยวกับนโยบายหรือหลักการในการเก็บข้อมูลของหน่วยงานของตน</u>*** ~~***ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม***~~

อี. ความไม่ชัดเจนของข้อกำหนดเรื่องความยินยอม

บีเอสเอยังคงมีความกังวลเป็นอย่างยิ่งว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอาจถูกตีความในลักษณะที่กำหนดหน้าที่ต่างหากให้แก่ผู้ควบคุมข้อมูลในการได้รับความยินยอมก่อนการใช้ข้อมูลแม้ว่าข้อมูลนั้นจะได้มาโดยชอบด้วยกฎหมายและโดยที่เจ้าของข้อมูลทราบว่าจะมีการใช้ข้อมูลเช่นนั้น นอกเหนือจากหน้าที่ตาม **มาตรา 19** ในการแจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับ*การเก็บรวบรวม*ข้อมูลส่วนบุคคลแล้ว **มาตรา 27** ก็มีความกำกวมและอาจถูกตีความไปได้ว่าเป็นหน้าที่ต่างหากที่จะต้องได้รับความยินยอมก่อน*ใช้หรือเปิดเผย*ข้อมูลนั้นในลักษณะใดๆ

เพื่อไม่ให้เกิดความกำกวม **มาตรา 27** ควรมีการแก้ไขให้ชัดเจนว่าเจ้าของข้อมูลสามารถให้ความยินยอมล่วงหน้าสำหรับการใช้ข้อมูลส่วนบุคคลของตนได้โดยการตกลงตามหรือไม่ปฏิเสธนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูล นอกจากนี้ ควรกำหนดไว้อย่างชัดเจนว่าผู้ควบคุมข้อมูลสามารถใช้ข้อมูลส่วนบุคคลในลักษณะที่เป็นไปตามข้อมูลที่ผู้ควบคุมข้อมูลได้ให้ไว้ หรือสอดคล้องกับบริบทของธุรกรรมหรือความคาดหมายตามควรของผู้บริโภค หรือในลักษณะอื่นที่อาจตรงตามวัตถุประสงค์แต่เดิมที่มีการเก็บรวบรวมข้อมูลนั้น

หากไม่แก้บทบัญญัติที่กำกวมนี้ให้มีความชัดเจน ข้อกำหนดนี้อาจขัดกับกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) และในทางปฏิบัติอาจทำให้การจัดให้บริการต่างๆ ในยุคปัจจุบันที่ต้องอาศัยข้อมูล อาทิเช่น คลาวด์คอมพิวติ้ง ไม่สามารถกระทำได้ กรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปคได้กำหนดระบบที่สมเหตุสมผลที่ช่วยให้แน่ใจได้ว่าผู้บริโภคจะได้รับแจ้งถึงประเภทข้อมูลที่ผลิตภัณฑ์

หรือบริการออนไลน์จะเก็บรวบรวมและจะใช้ข้อมูลนั้นอย่างไร หลักการในการแจ้งข้อมูลดังกล่าวจะช่วยให้ผู้บริโภคได้ทราบข้อมูลที่เกี่ยวข้องอย่างดีแล้วจึงตัดสินใจว่าตนจะยินยอมตามวิธีปฏิบัติเกี่ยวกับการเก็บรวบรวมข้อมูลของบริการออนไลน์หรือไม่ นอกจากนี้ กรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปคยอมรับว่าผู้ให้บริการออนไลน์อาจใช้ข้อมูลที่ตนเก็บรวบรวมจากผู้บริโภคได้เท่าที่การใช้นั้นสอดคล้องกับข้อกำหนดที่ระบุไว้ในหนังสือแจ้ง

อันที่จริงแล้ว กลไกที่จัดทำขึ้นเพื่อให้ผู้ใช้ให้ความยินยอมและควบคุมการเก็บรวบรวมและการใช้ข้อมูลของตนนั้นมีอยู่มากมาย ซึ่งกลไกที่ให้ผู้ใช้เลือกที่จะปฏิเสธไม่ให้ความยินยอม ซึ่งเป็นกลไกที่มีประสิทธิภาพมากกว่าสามารถให้ความคุ้มครองในเรื่องความเป็นส่วนตัวของผู้บริโภคได้ดีกว่า (อีกทั้งรบกวนผู้ใช้อินเทอร์เน็ตน้อยกว่า) กลไกที่ผู้ใช้ต้องเลือกให้ความยินยอม ซึ่งเป็นกลไกที่ด้อยกว่า

ข้อเสนอแนะ

เพื่อให้การตีความของ**มาตรา 27** สอดคล้องกับกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค บีเอสเอขอเรียนเสนอให้แก้ไขดังนี้

> ***มาตรา 27***
>
> ~~*ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26*~~ ***อาจใช้ โอน หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลนั้นได้เท่านั้น โดยต้องกระทำในลักษณะที่เป็นไปตามข้อมูลที่ผู้ควบคุมข้อมูลได้ให้ต่อเจ้าของข้อมูลไว้ตามมาตรา 23 และสอดคล้องกับบริบทของธุรกรรม หรือความคาดหมายตามควรของผู้บริโภค หรือในลักษณะอื่นที่อาจตรงตามวัตถุประสงค์แต่เดิมที่มีการเก็บรวบรวมข้อมูลนั้น เว้นแต่ในกรณีดังต่อไปนี้***
>
> 1. ***เจ้าของข้อมูลได้ให้ความยินยอมไว้***
> 2. ***การใช้หรือการเปิดเผยนั้นเป็นการจำเป็นต่อการจัดให้บริการหรือผลิตภัณฑ์ที่เจ้าของข้อมูลร้องขอ***
> 3. ***การใช้หรือการเปิดเผยนั้นเป็นการจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมาย หรือ***
> 4. ***ข้อมูลส่วนบุคคลนั้นได้เก็บรวบรวมตามมาตรา 24***

การโอนข้อมูลไปยังต่างประเทศ (มาตรา 16(5) และมาตรา 28-29)

เอ. เรื่องการโอนข้อมูลไปยังต่างประเทศควรมีกรอบกฎหมายและขั้นตอนที่ชัดเจนยิ่งขึ้น

I. กำหนดให้มีหลักเรื่องภาระรับผิดชอบ (Accountability) ไว้ในกรอบกฎหมายในเรื่องการโอนข้อมูลไปยังต่างประเทศ

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันกำหนดให้การมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเป็นเงื่อนไขสำคัญของการโอนข้อมูลไปยังต่างประเทศ การที่จะกำหนดให้คณะกรรมการจัดทำข้อตกลงในเรื่องมาตรฐานที่เพียงพอกับประเทศหรือเขตปกครองอื่นย่อมจะสร้างภาระอย่างมีนัยสำคัญแก่คณะกรรมการ ซึ่งในเรื่องข้อกำหนดเกี่ยวกับมาตรฐานที่เพียงพอนี้ เราได้มีประสบการณ์จากคำสั่งของสหภาพยุโรปเรื่องการคุ้มครองข้อมูลส่วนบุคคล (ซึ่งปัจจุบันรวมอยู่ใน GDPR) แล้ว ซึ่งแสดงให้เห็นถึงข้อเสียที่สำคัญหลายประการของการจัดให้มีข้อกำหนดดังกล่าว การตรวจสอบเรื่องมาตรฐานที่เพียงพอเป็นเรื่องที่ต้องใช้เวลาและทรัพยากรอย่างมหาศาล ด้วยเหตุนี้ สหภาพยุโรปจึงได้กำหนดในเรื่องมาตรฐานที่เพียงพอไว้เพียงเล็กน้อย นอกจากนี้ การตรวจสอบเรื่องมาตรฐานที่เพียงพอต้องมุ่งไปที่มาตรฐานกฎหมายที่เป็นกิจจะลักษณะ ซึ่งอาจไม่ได้ทำให้เห็นภาพรวมของการรักษาความมั่นคงปลอดภัยของประเทศนั้นได้ กล่าวอีกนัยหนึ่ง การที่ประเทศหนึ่งให้การคุ้มครองตามกฎหมายอย่างเป็นลายลักษณ์อักษรหรือเป็นกิจจะลักษณะไม่สามารถรับประกันได้ว่าการปฏิบัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้นจะมีมาตรฐานสูง

ด้วยเหตุนี้ บีเอสเอจึงเห็นว่าจะเป็นการสมควรอย่างยิ่งหากสภานิติบัญญัติจะได้พิจารณาว่าจะนำเรื่องภาระรับผิดชอบไปรวมอยู่ในกรอบกฎหมายในเรื่องการโอนข้อมูลไปยังต่างประเทศได้อย่างไร หลักในเรื่อง “ภาระรับผิดชอบ” หรือ Accountability มีการกำหนดไว้เป็นครั้งแรกในแนวทางการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ ขององค์กรเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-operation and Development: OECD)[12] และต่อมาได้รับการยอมรับและรวมไว้อยู่ในกรอบกฎหมายเรื่องการคุ้มครองข้อมูลส่วนบุคคลในทั่วโลก โดยวิธีดังกล่าวนี้เป็นการจัดการข้อมูลระหว่างประเทศที่คุ้มครองบุคคลได้อย่างมีประสิทธิภาพและทำให้การโอนของข้อมูลเป็นไปได้อย่างสม่ำเสมอและต่อเนื่อง หลักในเรื่องภาระรับผิดชอบเป็นหลักการที่กำหนดให้หน่วยงานที่เก็บและใช้ข้อมูลต้องมีความรับผิดชอบในการคุ้มครองข้อมูลและการใช้ข้อมูลนั้นอย่างเหมาะสม ไม่ว่าจะมีการประมวลผลข้อมูลนั้นที่ใดหรือโดยผู้ใด อีกทั้งกำหนดให้หน่วยงานที่โอนข้อมูลต้องดำเนินการที่จำเป็นเพื่อให้แน่ใจว่ามีการปฏิบัติหน้าที่ไม่ว่าจะเป็นหน้าที่ตามกฎหมาย แนวทาง หรือคำมั่นสัญญาที่เกี่ยวข้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ดังนั้น การพิจารณานำแนวคิดในเรื่องภาระรับผิดชอบมาใช้ใน**มาตรา 28** และ**มาตรา 29** โดย**กำหนดอย่างชัดเจนว่าผู้ควบคุมข้อมูลที่โอนข้อมูลไปยังต่างประเทศเป็นบุคคลที่ในที่สุดแล้วต้องรับผิดชอบในการคุ้มครองข้อมูลนั้นและในการใช้ข้อมูลนั้นอย่างเหมาะสมในประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลนั้น** จะสามารถคุ้มครองและส่งเสริมให้มีการใช้ข้อมูลส่วนบุคคลด้วยความรับผิดชอบได้อย่างมีประสิทธิภาพและเป็นประโยชน์ยิ่งกว่าการใช้หลักในเรื่องมาตรฐานที่เพียงพอ

นอกจากนี้ แม้หลักเกณฑ์ตาม**มาตรา 28 และมาตรา 16(5)** อาจเป็นประโยชน์โดยทั่วไป แต่การจัดทำมาตรการ แนวทาง กฎระเบียบ และวิธีการเกี่ยวกับข้อยกเว้นต่างๆ ให้มีความสอดคล้องกับวิธีปฏิบัติที่ดีและกรอบมาตรฐานที่สากลยอมรับมากที่สุดเท่าที่สามารถกระทำได้ก็เป็นเรื่องที่สำคัญอย่างยิ่ง ด้วยสภาพเศรษฐกิจดิจิทัลในทั่วโลก จำเป็นอย่างยิ่งที่รัฐบาลจะต้องดำเนินการให้แน่ใจว่าการโอนข้อมูลระหว่างประเทศสามารถเกิดขึ้นได้อย่างอิสระ อีกทั้งต้องไม่กำหนดข้อจำกัดในการโอนข้อมูลระหว่างประเทศที่ไม่ได้มีความจำเป็นหรือ

[12] ที่ www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

ก่อให้เกิดภาระหน้าที่ การกำหนดให้มีข้อจำกัดในการโอนข้อมูลระหว่างประเทศที่ก่อให้เกิดภาระหน้าที่เป็นเรื่องที่ไม่สมควรกระทำอย่างยิ่ง บีเอสเอขอสนับสนุนให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้อย่างชัดเจนว่าผู้ควบคุมข้อมูลสามารถโอนข้อมูลไปยังต่างประเทศได้โดยอิสระตราบเท่าที่ผู้ควบคุมข้อมูลสามารถคุ้มครองข้อมูลนั้นได้หรือปฏิบัติตามวิธีปฏิบัติที่สากลยอมรับ เช่น พันธสัญญาที่จะปฏิบัติตามแนวทางในการคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดนของเอเปค (Cross-Border Privacy Rules)

II. การโอนข้อมูลไม่ควรต้องได้รับความเห็นชอบจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก่อน

มาตรา 28 และมาตรา 29 ส่งผลให้การโอนข้อมูลไปยังต่างประเทศและองค์การระหว่างประเทศ ซึ่งรวมถึงการโอนข้อมูลภายในองค์กรเดียวกันที่อยู่ในต่างประเทศ ต้องได้รับการตรวจสอบและรับรองจากสำนักงาน[13] กล่าวคือ

- **มาตรา 28 วรรคหนึ่ง** อนุญาตให้มีการโอนข้อมูลส่วนบุคคลได้หากมี “มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ” ทั้งนี้ “*ตามที่คณะกรรมการประกาศกำหนด*” แต่ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันยังไม่เป็นที่แน่ชัดว่า “การประกาศกำหนด” นั้นจะกระทำเป็นรายกรณีไปหรือไม่ และโดยทั่วไปองค์กรต้องได้รับความเห็นชอบก่อนการโอนข้อมูลไปยังต่างประเทศหรือไม่
- นอกจากนี้ **มาตรา 29 วรรคหนึ่ง** กำหนดให้องค์กรต่างๆ ต้องส่งนโยบายของตนในการคุ้มครองข้อมูลส่วนบุคคลไปให้สำนักงานตรวจสอบและรับรองก่อนทำการโอนข้อมูลภายในองค์กรเดียวกันที่อยู่ในต่างประเทศ
- **มาตรา 29 วรรคสอง** กำหนดให้ลักษณะของ “เครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน” และหลักเกณฑ์และวิธีการรับรอง ต้องเป็นไปตามที่คณะกรรมการประกาศกำหนด
- นอกจากนี้ **มาตรา 29 วรรคสาม** บัญญัติว่าในกรณีที่ยังไม่ได้รับความเห็นชอบจากคณะกรรมการ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้หากมีการบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลและมาตรการเยียวยาที่เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด แต่ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันยังไม่เป็นที่แน่ชัดว่าการประกาศกำหนดและความเห็นชอบของคณะกรรมการจะต้องกระทำเป็นรายกรณีก่อนการโอนข้อมูลแต่ละครั้งหรือไม่

การกำหนดให้คณะกรรมการต้องให้ความเห็นชอบก่อนการโอนข้อมูลไปยังต่างประเทศแต่ละครั้ง หรือรับรองนโยบาย “ในการคุ้มครองข้อมูลส่วนบุคคล” สำหรับการโอนข้อมูลภายในองค์กรเดียวกัน ย่อมจะสร้างภาระอย่างยิ่งแก่คณะกรรมการ นอกจากนี้ยังเป็นขั้นตอนที่ยุ่งยากและไม่จำเป็น ในทางปฏิบัติ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลซึ่งทำงานบนโซลูชั่นที่ใช้อินเทอร์เน็ตหรือคลาวด์คอมพิวติ้งเป็นหลักย่อมไม่สามารถขอความ

[13] มาตรา 29 วรรคหนึ่ง อธิบายการโอนข้อมูลภายในองค์กรเดียวกันว่าเป็นการส่งหรือโอน “. . .*ข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศ และอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน*. . .”

เห็นชอบสำหรับการโอนข้อมูลไปยังทุกประเทศหรือองค์กรที่จะส่งข้อมูลไปนั้นได้ ข้อกำหนดนี้จะทำให้การให้บริการดิจิทัลแก่ผู้บริโภคในประเทศไทยโดยบริษัทต่างๆ ล่าช้าลงอย่างยิ่ง

III. การบัญญัติเรื่องภาระรับผิดชอบในมาตรา 29 วรรคสามไว้อย่างชัดเจน

ตาม**มาตรา 29** การโอนข้อมูลภายในองค์กรเดียวกันสามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามข้อกำหนดเรื่องมาตรฐานที่เพียงพอใน**มาตรา 28** โดยมีเงื่อนไขว่าการโอนข้อมูลนั้นเป็นไปตามข้อกำหนดใน**มาตรา 29** อย่างไรก็ดี **มาตรา 29 วรรคสาม** ได้กำหนดวิธีการสำหรับการโอนข้อมูลไปยังต่างประเทศในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการตาม**มาตรา 28** และยังไม่มีนโยบายตาม**มาตรา 29 วรรคหนึ่ง** ซึ่งอาจทำให้ร่างพระราชบัญญัติฉบับนี้มีความกำกวมและก่อให้เกิดความสับสนว่าคำวินิจฉัยของคณะกรรมการตาม**มาตรา 28** ใช้กับการโอนข้อมูลภายในองค์กรเดียวกันที่เป็นไปตามข้อกำหนดในมาตรา 29 ด้วยหรือไม่

นอกจากนี้ ถ้อยคำใน**มาตรา 29 วรรคสาม** ยังอาจก่อให้เกิดความสับสนว่าผู้ประมวลผลข้อมูลมีหน้าที่ในการดูแลให้การโอนข้อมูลไปยังต่างประเทศเป็นไปตาม**มาตรา 28** และหลักเกณฑ์ที่จะประกาศกำหนดตาม**มาตรา 16(5)** หรือไม่ ซึ่งขัดกับถ้อยคำใน**มาตรา 28** เอง ที่มีการระบุไว้อย่างชัดเจนว่าผู้ควบคุมข้อมูลมีหน้าที่รับผิดชอบดังกล่าว ไม่ใช่ผู้ประมวลผลข้อมูล การกำหนดให้ผู้ประมวลผลข้อมูลมีความรับผิดโดยตรงหรือร่วมกันกับผู้ควบคุมข้อมูลจะทำให้เกิดความสับสนในหลักเรื่องภาระรับผิดชอบ นอกจากนี้ โดยทั่วไปแล้วผู้ประมวลผลข้อมูลไม่ได้มีความสัมพันธ์โดยตรงกับเจ้าของข้อมูลหรือไม่ทราบประเภทข้อมูลที่ตนกำลังให้บริการประมวลผลในนามของลูกค้า อันทำให้ผู้ประมวลผลข้อมูลไม่อาจทราบได้ว่าข้อมูลที่โอนไปยังต่างประเทศเป็นข้อมูลส่วนบุคคลหรือไม่ ซึ่งหากเป็น จะต้องให้สำนักงานและคณะกรรมการตรวจสอบและรับรอง

ด้วยเหตุนี้ จึงจำเป็นอย่างยิ่งที่ต้องจัดทำให้ประเด็นต่อไปนี้มีความชัดเจน

เอ. คำวินิจฉัยของคณะกรรมการตาม**มาตรา 28** **ไม่ใช้กับการโอนข้อมูลไปยังองค์กรเดียวกันที่อยู่ในต่างประเทศ** ที่เป็นไปตามข้อกำหนดในมาตรา 29 และ

บี. **มาตรา 29 วรรคสาม** ใช้กับทั้ง**คำวินิจฉัยเกี่ยวกับการโอนข้อมูลไปยังต่างประเทศตามมาตรา 28 และมาตรา 29 วรรคหนึ่ง**

ข้อเสนอแนะ

ในประเด็นข้อกังวลที่เรียนข้างต้นนี้ เพื่อให้สอดคล้องกับวิธีปฏิบัติที่ดีที่สากลยอมรับ **บีเอสเอเห็นว่าควรนำหลักเรื่องภาระรับผิดชอบ (Accountability) มาใช้อย่างเต็มที่กับเรื่องการโอนข้อมูลไปยังต่างประเทศและกำหนดกรอบกฎหมายสำหรับการโอนข้อมูลไปยังต่างประเทศไว้อย่างชัดเจน**โดยการแก้ไขดังนี้

(เอ) แก้ไข**มาตรา 28** ให้มีความชัดเจนว่าผู้ควบคุมข้อมูลที่ทำการโอนข้อมูลไปยังต่างประเทศเป็นบุคคลที่ในที่สุดแล้วต้องรับผิดชอบในการจัดให้มีการคุ้มครองข้อมูลและการใช้ข้อมูลที่เหมาะสมในประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลนั้น และสำหรับการโอนข้อมูลระหว่างองค์กรเดียวกันที่อยู่ในต่างประเทศ ดังนั้น ผู้ควบคุมข้อมูลที่ได้ดำเนินการอย่างเหมาะสมเพื่อให้แน่ใจว่ามีการคุ้มครอง

เพียงพอหรือได้มีมาตรการรักษาความปลอดภัยที่เหมาะสมซึ่งให้การคุ้มครองได้ในระดับเดียวกันแล้ว จะต้องสามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้

(บี) กำหนดอย่างชัดเจนว่าขั้นตอนที่กล่าวไว้ในข้อ II ในส่วนนี้ไม่ต้องได้รับความเห็นชอบจากสำนักงานก่อน

- กล่าวโดยเฉพาะ สำหรับการโอนข้อมูลภายในองค์กร **<u>ควรตัดมาตรา 29 วรรคหนึ่งและวรรคสองออกทั้งหมด</u>** และนำหลักในเรื่องภาระรับผิดชอบมาใช้อย่างเต็มที่กับการโอนข้อมูลไปยังต่างประเทศ โดยอาจอนุญาตให้การโอนข้อมูลภายในองค์กรที่เป็นไปตามข้อกำหนดใน**มาตรา 28** สามารถกระทำได้
- อย่างไรก็ดี หากสภานิติบัญญัติเห็นควรให้คงกรอบกฎหมายในการตรวจสอบและประกาศกำหนดสำหรับการโอนข้อมูลภายในองค์กรไว้ **<u>กรอบกฎหมายดังกล่าวควรเป็นเพียงทางเลือกเพิ่มเติมจากกลไกในมาตรา 28 สำหรับการโอนข้อมูลไปยังต่างประเทศ กรอบกฎหมายนี้ไม่ควรใช้กับทุกกรณีของการโอนข้อมูลภายในองค์กร</u>**

(ซี) แก้ไข**มาตรา 28** ให้มีความชัดเจนว่า ในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการตาม**มาตรา 28** ผู้ควบคุมข้อมูลสามารถโอนข้อมูลได้หากเป็นการโอนโดยใช้วิธีการที่ประกาศกำหนดโดยคณะกรรมการ ซึ่งต้องเป็นไปตามกรอบมาตรฐานการคุ้มครองข้อมูลที่สากลยอมรับ

เพื่อให้บรรลุผลข้างต้น **มาตรา 28** ควรแก้ไขดังนี้ และควรตัด**มาตรา 29** ออกไป

มาตรา 28

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ***<u>ผู้ควบคุมข้อมูลต้องดำเนินการที่เหมาะสมเพื่อให้แน่ใจว่า</u>****ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16(5)* ***<u>หรือผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการคุ้มครองที่เหมาะสมซึ่งมีมาตรฐานสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนนั้นเทียบเท่ากับการคุ้มครองตามพระราชบัญญัตินี้</u>*** *เว้นแต่*

. . .

ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

<u>ในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการตามมาตรา 28 ผู้ควบคุมข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้เมื่อผู้ควบคุมข้อมูลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมแล้ว ทั้งนี้ โดยที่ไม่ต้องได้รับความเห็นชอบเป็นการเฉพาะเจาะจงจากคณะกรรมการก่อน</u>

บี. จัดให้มีช่องทางเพิ่มเติมสำหรับการโอนข้อมูลส่วนบุคคลที่เป็นที่ชัดเจนว่าเป็นไปตามกรอบมาตรฐานและวิธีปฏิบัติที่ดีที่สากลยอมรับ

บีเอสเอเห็นว่ากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*ไม่*ควรมีข้อจำกัดในสาระสำคัญเกี่ยวกับการโอนข้อมูลระหว่างประเทศ และควรมีกลไกสำหรับการโอนข้อมูลที่ชัดเจน มีความยืดหยุ่น และสอดคล้องกับวิธีปฏิบัติที่ดีและกรอบมาตรฐานที่สากลยอมรับ อนึ่ง การโอนข้อมูลระหว่างประเทศมักต้องไปเป็นตามพันธสัญญาที่มีตามข้อตกลงความร่วมมือระหว่างประเทศ ตลอดจนประมวลจริยธรรมหรือกรอบกฎเกณฑ์ของอุตสาหกรรมที่จัดทำขึ้นโดยผู้มีส่วนได้เสียหลากหลายฝ่ายตามขั้นตอนที่โปร่งใส อันเป็นการรับประกันเพิ่มเติมว่าบริษัทต่างๆ จะคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

การแก้ไขมาตรา 28-29 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลตามที่เรียนเสนอนี้เป็นเพียงกลไกเพิ่มเติมสำหรับการโอนข้อมูลระหว่างประเทศ อย่างไรก็ดี ไม่มีกลไกสำหรับการโอนข้อมูลใดที่จะใช้เพียงลำพังโดยที่สามารถตอบโจทย์ตามความต้องการของเทคโนโลยีและบริการในยุคปัจจุบันได้

ข้อเสนอแนะ

บีเอสเอขอเรียนเน้นย้ำว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรยอมรับอย่างชัดแจ้งให้มีกลไกเพิ่มเติมสำหรับการโอนข้อมูลที่ทำให้บริษัทสามารถใช้วิธีการคุ้มครองอื่นๆ ที่มีผลผูกพันตามกฎหมายได้ ซึ่งรวมถึง

(เอ) **วิธีปฏิบัติที่ดี การรับรอง และมาตรฐานที่สากลยอมรับ** บริษัทที่ตกลงตามวิธีปฏิบัติที่ดีที่ใช้ในทั่วโลกและ/หรือได้รับการรับรองตามมาตรฐานที่สากลยอมรับย่อมเป็นสัญญาณที่แสดงให้เห็นว่าบริษัทเหล่านี้มีหน้าที่ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับข้อมูลส่วนบุคคลที่มีการโอนระหว่างประเทศ ด้วยเหตุนี้ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจึงสมควรกำหนดว่าการที่องค์กรที่ปฏิบัติตามวิธีปฏิบัติที่ดีหรือได้รับการรับรองตามมาตรฐานดังกล่าวถือเป็นการปฏิบัติตามข้อกำหนดในเรื่องการโอนข้อมูลไปยังต่างประเทศตามร่างพระราชบัญญัตินี้แล้ว ทั้งนี้ มาตรฐานที่สากลยอมรับนี้ควรรวมถึงกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรและข้อสัญญามาตรฐานเพื่อการคุ้มครองข้อมูล ตาม GDPR[14] และแนวทางในการคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดนของเอเปค

(บี) **หลักเกณฑ์อื่น ๆ ที่อนุญาตให้สามารถโอนข้อมูลได้** หากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลปรับใช้หลักเกณฑ์ตามข้อ 46 แห่ง GDPR ในการอนุญาตให้สามารถโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักรได้จะเป็นการสมควรอย่างยิ่ง กล่าวคือ บีเอสเอเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรกำหนดให้ข้อสัญญามาตรฐานตามที่ GDPR อนุญาต กฎเกณฑ์การคุ้มครองข้อมูล

[14] ออกตามข้อ 47 และข้อ 93(2) ของระเบียบทั่วไปแห่งสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (GDPR) ตามลำดับ

ส่วนบุคคลภายในองค์กร และแนวปฏิบัติที่ได้รับความเห็นชอบ เป็นหลักเกณฑ์เพิ่มเติมที่อนุญาตให้สามารถโอนข้อมูลระหว่างประเทศได้

การแจ้งเหตุการละเมิดข้อมูล (มาตรา 36(4))

บีเอสเอเห็นว่าควรมีระบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่ใช้ได้กับธุรกิจและองค์กรทั้งหมด การจัดให้มีบทบัญญัติเรื่องการละเมิดข้อมูลที่ร่างขึ้นอย่างเหมาะสมจะช่วยส่งเสริมให้มีการใช้วิธีปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีประสิทธิภาพ อีกทั้งทำให้บุคคลสามารถดำเนินการเพื่อปกป้องตนเองได้ในกรณีที่ข้อมูลของตนมีความเสี่ยงว่าจะถูกละเมิด ในการจัดทำบทบัญญัติเรื่องการแจ้งเหตุการละเมิดข้อมูล เป็นเรื่องจำเป็นอย่างยิ่งที่ต้องเข้าใจว่าการละเมิดข้อมูลแต่ละกรณีไม่ได้ทำให้เกิดภัยคุกคามในระดับเดียวกันทั้งหมด และในหลายกรณี การละเมิดข้อมูลไม่ได้ก่อให้เกิดความเสี่ยงขึ้นจริงๆ ต่อบุคคลที่ข้อมูลถูกละเมิด

เพื่อให้ผู้บริโภคไม่ต้องได้รับการแจ้งมากเกินไปเกี่ยวกับการละเมิดข้อมูลที่ไม่มีความสำคัญ หน้าที่ในการแจ้งควรมีเฉพาะในกรณีที่มีความเสี่ยงอย่างยิ่งที่จะเกิดความเสียหายต่อผู้ใช้[15] อย่างไรก็ดี ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันไม่ได้กำหนดข้อยกเว้นของหน้าที่ในการแจ้งไว้ ซึ่งไม่สอดคล้องกับวิธีปฏิบัติสากล และอาจทำให้มีการแจ้งมากเกินไปและทำให้ผู้ใช้เบื่อหน่ายและไม่ให้ความสนใจต่อการแจ้งอีกต่อไป อันทำให้ข้อกำหนดเรื่องการแจ้งเหตุการละเมิดต่อเจ้าของข้อมูลมีประโยชน์ลดลง ดังนั้น อาจเป็นการสมควรที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะกำหนดให้มีข้อยกเว้นที่เหมาะสมของหน้าที่ในการแจ้งเหตุการละเมิดที่สอดคล้องกับวิธีปฏิบัติสากล กล่าวโดยเฉพาะ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรกำหนดให้มีข้อยกเว้นของข้อกำหนดเรื่องการแจ้งต่อไปนี้เป็นอย่างน้อย

เอ. ในกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้ใช้มาตรการทางเทคนิคและมาตรการในองค์กรที่เหมาะสม เช่น โดยการทำให้ข้อมูลส่วนบุคคลไม่สามารถเป็นที่เข้าใจได้สำหรับบุคคลใดๆ ที่ไม่มีอำนาจในการเข้าถึงข้อมูลนั้น

บี. ในกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้ใช้มาตรการที่ทำให้มั่นใจได้ว่าความเสี่ยงว่าจะเกิดความเสียหายนั้นไม่มีอยู่อีกต่อไป

ซี. ในกรณีที่การแจ้งต้องใช้ความพยายามเกินควรหากต้องทำการแจ้งให้แต่ละบุคคลทราบ ซึ่งในกรณีดังกล่าว ควรจัดให้มีการสื่อสารต่อสาธารณชนหรือมาตรการในทำนองเดียวกันที่มีประสิทธิภาพเท่าเทียมกันในการทำให้เจ้าของข้อมูลได้รับการแจ้ง

---

[15] วิธีการที่มีการใช้ในระดับสากลเพื่อให้หน้าที่ในการแจ้งเหตุการละเมิดมีเฉพาะในกรณีมีความเสี่ยงอย่างร้ายแรงว่าจะเกิดความเสียหาย เช่น

- กฎหมายว่าด้วยความเป็นส่วนตัวของออสเตรเลีย ค.ศ. 1998 (ที่แก้ไขเพิ่มเติม ปี ค.ศ. 2017) มาตรา 26WA: “น่าจะส่งผลให้เกิดความเสียหายอย่างร้ายแรง”
- กฎหมายแคนาดาว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (ค.ศ. 2015) มาตรา 10.1 (1): “มีความเสี่ยงอย่างแน่ชัดว่าจะเกิดความเสียหายอย่างร้ายแรงต่อบุคคล”
- กฎหมายฟิลิปปินส์ว่าด้วยความเป็นส่วนตัวของข้อมูล ปี ค.ศ. 2012 มาตรา 20 “น่าจะก่อให้เกิดความเสี่ยงอย่างแน่ชัดว่าจะเกิดความเสียหายอย่างร้ายแรงต่อเจ้าของข้อมูลที่ได้รับผลกระทบ”
- GDPR ข้อ 33 การแจ้งจำเป็นต้องกระทำเว้นแต่การละเมิดข้อมูลส่วนบุคคลนั้น “ไม่น่าก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา”

ดี. ในกรณีที่กฎหมายอื่นที่ใช้บังคับได้กำหนดหน้าที่ที่ไม่สอดคล้องกัน หรือ

อี. ในกรณีที่การแจ้งอาจกระทบต่อกระบวนการสอบสวนเพื่อบังคับสิทธิที่กำลังดำเนินอยู่หรือจะดำเนินขึ้นโดยหน่วยงานบังคับใช้กฎหมายที่มีอำนาจ

ประการสุดท้าย เพื่อให้แน่ใจว่าเจ้าของข้อมูลจะได้รับการแจ้งที่สำคัญเมื่อเกิดเหตุการละเมิดข้อมูล เป็นเรื่องสำคัญอย่างยิ่งที่ผู้ควบคุมข้อมูลต้องมีเวลาเพียงพอในการประเมินความเสี่ยงอย่างละเอียดถี่ถ้วนเพื่อจะได้ทราบขอบเขตของความเสี่ยงต่อความมั่นคงปลอดภัยและป้องกันไม่ให้มีการเปิดเผยข้อมูลอื่นต่อไป ดังนั้น การกำหนดให้บทบัญญัติเรื่องการแจ้งเหตุการละเมิดมีระยะเวลาที่ตายตัวสำหรับการแจ้งจึงอาจทำให้บทบัญญัติดังกล่าวเสื่อมประสิทธิภาพลงได้

ข้อเสนอแนะ

มาตรา 36(4) ควรแก้ไขเพื่อให้กรอบกฎหมายในเรื่องการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่เสนอนี้ (1) ทำให้เจ้าของข้อมูลได้รับการแจ้งที่สำคัญ (2) ทำให้ผู้ควบคุมข้อมูลสามารถมุ่งไปที่การจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่เกิดขึ้นในขณะนั้นๆ และป้องกันไม่ให้เกิดการเปิดเผยข้อมูลอื่นต่อไป และ (3) ทำให้เกิดความชัดเจนในเรื่องความรับผิดและหน้าที่ความรับผิดชอบในกรณีที่มีการละเมิดข้อมูล **มาตรา 36(4)** ตามที่เสนอนี้จะทำให้บรรลุผลต่อไปนี้ได้

(เอ) **มีมาตรการที่คำนึงถึงความเสี่ยงเป็นสำคัญ ซึ่งทำให้หน้าที่ในการแจ้งเหตุการละเมิดข้อมูลเกิดขึ้นต่อเมื่อเกิดการละเมิดที่จะ "ทำให้มีความเสี่ยงอย่างมีนัยสำคัญว่าจะเกิดความเสียหาย"** เพื่อให้มีความสมดุลยิ่งขึ้นระหว่างจำนวนและประเภทของการแจ้งที่เจ้าของข้อมูลจะได้รับ และป้องกันไม่ให้เจ้าของข้อมูลเบื่อหน่ายกับการได้รับการแจ้ง นอกจากนี้ **การละเมิดข้อมูลที่ถูกเข้ารหัสหรือข้อมูลที่ไม่สามารถเข้าใจได้ไม่ควรต้องมีหน้าที่ในการแจ้งเหตุการละเมิด**

(บี) **กำหนดเหตุที่ก่อให้เกิดหน้าที่ในการแจ้งทันที "โดยไม่ชักช้า"** เพื่อสร้างความยืดหยุ่นให้แก่ผู้ควบคุมข้อมูลในการจัดการทรัพยากรและสิ่งที่ต้องให้ความสำคัญในทันทีภายหลังการละเมิด

(ซี) มี**ข้อยกเว้นหน้าที่ในการแจ้งเหตุการละเมิดข้อมูล**ตามที่กล่าวไว้ข้างต้น

บีเอสเอขอเรียนเสนอให้แก้ไข**มาตรา 36(4)** ดังนี้

> ***มาตรา 36***
>
> *. . .*
>
> *(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า**ในกรณีที่การละเมิดนั้นอาจทำให้มีความเสี่ยงอย่างมีนัยสำคัญว่าจะเกิดความเสียหาย** ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคล**ที่ทำให้มีความเสี่ยงอย่างมีนัยสำคัญว่าจะเกิดความเสียหายและเป็นการละเมิดข้อมูลส่วนบุคคล**เกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนว*

ทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

อย่างไรก็ดี ผู้ควบคุมข้อมูลไม่มีหน้าที่ในการแจ้งในกรณีดังต่อไปนี้

ก. ข้อมูลที่ถูกละเมิดมีการจัดเก็บในลักษณะที่ทำให้บุคคลภายนอกที่ไม่มีอำนาจในการเข้าถึงข้อมูลนั้นไม่สามารถทำไปใช้ได้ อ่านไม่ได้ หรือไม่สามารถเข้าใจได้ ตามวิธีปฏิบัติหรือวิธีการที่เป็นที่ยอมรับอย่างกว้างขวางว่าเป็นวิธีปฏิบัติของอุตสาหกรรมหรือมาตรฐานของอุตสาหกรรมที่มีประสิทธิภาพ

ข. ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้ใช้มาตรการที่ทำให้มั่นใจได้ว่าความเสี่ยงที่จะเกิดความเสียหายนั้นไม่มีอยู่อีกต่อไป

ค. จะต้องใช้ความพยายามเกินควรหากต้องทำการแจ้งให้แต่ละบุคคลทราบ ซึ่งในกรณีดังกล่าวควรจัดให้มีการสื่อสารต่อสาธารณชนหรือมาตรการในทำนองเดียวกันที่มีประสิทธิภาพเท่าเทียมกันในการทำให้เจ้าของข้อมูลได้รับการแจ้ง

ง. กฎหมายอื่นที่ใช้บังคับได้กำหนดหน้าที่ที่ไม่สอดคล้องกัน หรือ

จ. การแจ้งอาจกระทบต่อกระบวนการสอบสวนเพื่อบังคับสิทธิที่กำลังดำเนินอยู่หรือจะดำเนินขึ้นโดยหน่วยงานบังคับใช้กฎหมายที่มีอำนาจ

ข้อกำหนดเรื่องความยินยอมกรณีผู้เยาว์ คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ (มาตรา 20)

เพื่อให้สอดคล้องกับ GDPR และกฎหมายสหรัฐอเมริกาว่าด้วยการคุ้มครองความเป็นส่วนตัวทางออนไลน์ของเด็ก (**COPPA**)[16] บีเอสเอจึงเห็นว่าเป็นการสมควรที่จะถือว่าข้อมูลส่วนบุคคลของเด็กเป็นข้อมูลที่มีความละเอียดอ่อนและต้องได้รับการคุ้มครองในระดับที่สูงขึ้น อย่างไรก็ดี ร่างพระราชบัญญัตินี้กำหนดอายุขั้นสูงไว้ที่ 20 ปี[17] ซึ่งขัดกับมาตรฐานอื่นเกี่ยวกับการคุ้มครองข้อมูลของเด็ก ตัวอย่างเช่น COPPA ใช้กับเด็กอายุต่ำกว่า 13 ปี โดยให้การคุ้มครองที่เหมาะสมแก่บุคคลในวัยที่เปราะบางเป็นพิเศษ สำหรับ GDPR กำหนดอายุขั้นสูงไว้ที่ 16 ปี แต่อนุญาตให้รัฐสมาชิกกำหนดอายุไว้ต่ำกว่านั้นได้ถึง 13 ปี[18] การที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลบัญญัติไว้ขัดกับ COPPA และ GDPR โดยเฉพาะการกำหนดให้กฎหมายให้การคุ้มครองในระดับสูงขึ้นแก่ผู้เยาว์ที่มีอายุมากกว่าตามที่กำหนดไว้ใน COPPA และ GDPR มาก อาจเป็นการกีดกันไม่ให้เยาวชนโดยเฉพาะวัยรุ่นตอนกลางและตอนปลาย สามารถเข้าถึงบริการที่เป็นประโยชน์ ในประเด็นนี้ บีเอสเอเห็นว่าการกำหนดอายุของเด็กเพื่อวัตถุประสงค์ในการให้การคุ้มครองในระดับสูงขึ้นไว้ที่ 13 ปี จะสามารถให้การ

[16] *ดูเพิ่มเติมได้ที่* 15 U.S.C. มาตรา 6501 และมาตราอื่นๆ ถัดจากนั้น และ 16 C.F.R. ส่วนที่ 314

[17] ประมวลกฎหมายแพ่งและพาณิชย์ไทย มาตรา 19

[18] ดู GDPR ข้อ 8(1)

คุ้มครองที่เพียงพอสำหรับเด็กวัยเยาว์ซึ่งมีความเปราะบางเป็นพิเศษได้ ในขณะที่ทำให้ผู้เยาว์ที่โตกว่าได้รับประโยชน์จากบริการที่เกี่ยวข้องกับข้อมูลได้อย่างง่ายดายด้วย

สิทธิอื่น ๆ ของผู้บริโภคและกลไกเรื่องภาระรับผิดชอบ (มาตรา 31, 32, 33 และ 38)

บีเอสเอเห็นด้วยอย่างยิ่งกับการให้อำนาจมากขึ้นแก่บุคคลในการควบคุมข้อมูลของตน โดยในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้มีบทบัญญัติเกี่ยวกับสิทธิของผู้บริโภคเพิ่มเติมขึ้น ซึ่งสอดคล้องกับวิธีปฏิบัติที่ดีที่สากลยอมรับ สิทธิดังกล่าวรวมถึงสิทธิในการขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตน (มาตรา 31) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน (มาตรา 32) และสิทธิในการทำลายหรือระงับการประมวลผลข้อมูลส่วนบุคคลชั่วคราว (มาตรา 33) อีกทั้งมีกลไกเรื่องภาระรับผิดชอบ เช่น การกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลบันทึกรายการการประมวลผลข้อมูล (มาตรา 38) เหล่านี้ล้วนทำให้บรรลุผลในเรื่องการให้อำนาจมากขึ้นแก่บุคคลในการควบคุมข้อมูลของตน สิทธิและกลไกเรื่องภาระรับผิดชอบเหล่านี้เป็นพื้นฐานสำคัญสำหรับการจัดทำกรอบการคุ้มครองข้อมูลที่มีประสิทธิภาพของประเทศไทย แต่ในขณะเดียวกัน เป็นเรื่องสำคัญยิ่งที่ระเบียบหรือประกาศที่จะออกตามร่างพระราชบัญญัตินี้ต้องมีความยืดหยุ่นและไม่เป็นการบังคับจนเกินไป มิฉะนั้นแล้ว หน้าที่เหล่านี้จะกลับสร้างปัญหาในทางปฏิบัติ ทำให้ต้นทุนในการปฏิบัติตามกฎระเบียบสูงขึ้น และลดแรงจูงใจที่ธุรกิจในประเทศไทยจะใช้ข้อมูลและเทคโนโลยีในรูปแบบใหม่ๆ

นอกจากนี้ สิทธิบางประการ เช่น ข้อกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัตินั้น (**มาตรา 31**) ควรลดหย่อนลงโดยการอนุญาตให้ผู้ควบคุมข้อมูลกำหนดวิธีการและรูปแบบที่กระทำได้ในทางปฏิบัติและเหมาะสมในทางเทคนิคได้เอง นอกจากนี้ ข้อกำหนดให้ผู้ควบคุมข้อมูลส่งข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง (**มาตรา 31(2)**) อาจทำให้เกิดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อีกทั้งอาจกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลได้

ด้วยเหตุนี้ บีเอสเอจึงเห็นว่าการบัญญัติในเรื่องสิทธิเหล่านี้ควรกระทำอย่างรอบคอบ โดยคณะกรรมการควรหารืออย่างเปิดเผยกับภาคอุตสาหกรรมเมื่อจัดทำแนวทาง ประกาศ และกฎหมายลำดับรองที่เกี่ยวข้องกับร่างพระราชบัญญัตินี้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 40)

หลักเกณฑ์ที่ทำให้มีความจำเป็นต้องจัดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรเป็นหลักเกณฑ์ที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับอื่นๆ นอกจากนี้ ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรกำหนดให้ชัดเจนว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่จำเป็นต้องอยู่ในประเทศไทย และเครือกิจการ (หรือเครือธุรกิจ) หนึ่งๆ สามารถแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขึ้นเพียงรายเดียวก็ได้ ทั้งนี้เพื่อให้บริษัทในเครือเดียวกันสามารถจัดทำและใช้มาตรฐานเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกันได้ แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้อยู่ทั่วโลกจะมีความเหลื่อมล้ำกันมากขึ้นเรื่อยๆ ก็ตาม ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันไม่ได้มีการกำหนดในเรื่องนี้

ข้อเสนอแนะให้มีการเปลี่ยนแปลงประการนี้จะทำให้ข้อกำหนดในร่างพระราชบัญญัติฯ มีความสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับอื่นๆ เช่น GDPR

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดว่า ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ และเจ้าของข้อมูลสามารถติดต่อกับทั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในเรื่องเกี่ยวกับสิทธิของตนได้ ข้อกำหนดนี้อาจไม่เหมาะกับผู้ประมวลผลข้อมูลที่มีข้อมูลอย่างจำกัดหรือไม่มีข้อมูลที่จะทำให้ทราบได้เลยว่าข้อมูลที่ตนกำลังประมวลผลอยู่นั้นเป็นข้อมูลส่วนบุคคลตามขอบเขตของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหรือไม่ และไม่ได้ติดต่อหรือมีความสัมพันธ์กับเจ้าของข้อมูล (เช่น ผู้ให้บริการคลาวด์) หน้าที่ของผู้ประมวลผลข้อมูลจึงควรมุ่งเน้นที่การวางมาตรการด้านการรักษาความปลอดภัยของระบบให้เหมาะสมตามเหตุผลอันสมควร

อำนาจของคณะกรรมการ (มาตรา 8-18 และมาตรา 88) สำนักงาน และคณะกรรมการผู้เชี่ยวชาญ (มาตรา 69-74)

บีเอสเอสเห็นเป็นการสมควรอย่างยิ่งที่ประเทศไทยผลักดันการจัดตั้งหน่วยงานที่มีอำนาจในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเพียงหน่วยงานเดียว เพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลและเพื่อกำกับดูแลการบังคับใช้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ดี บีเอสเอมีความกังวลที่บทบัญญัติบางประการอาจเป็นการให้อำนาจแก่คณะกรรมการและคณะกรรมการผู้เชี่ยวชาญที่แต่งตั้งขึ้นตาม**มาตรา 69** ไว้อย่างกว้างเกินไป ซึ่งรวมถึงอำนาจอันไม่มีข้อจำกัดของคณะกรรมการที่สามารถ *"กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้"* (**มาตรา 16(3)**)

นอกจากนี้ **มาตรา 70(2)** ยังให้อำนาจอย่างไม่จำกัดแก่คณะกรรมการผู้เชี่ยวชาญในการตรวจสอบหรือพิจารณา "การกระทำ*ใดๆ* เกี่ยวกับข้อมูลส่วนบุคคล" ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล เกี่ยวกับข้อมูลส่วนบุคคล อีกทั้ง**มาตรา 73** ยังให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญในการสั่งการให้มีการส่งเอกสาร ซึ่งไม่ใช่เพียงเพื่อวัตถุประสงค์ในการสอบสวนเรื่องที่มีผู้ร้องเรียน แต่ครอบคลุมไปถึง "*เรื่องอื่นใด*" ที่คณะกรรมการผู้เชี่ยวชาญอาจเห็นสมควร

นอกเหนือไปจากอำนาจในการตรวจสอบและเรื่องอื่นๆ แล้ว บทบัญญัติใน**มาตรา 72** ยังให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญในการลงโทษองค์กรต่างๆ หากพบว่าองค์กรเหล่านั้นปฏิบัติไม่ถูกต้องตามกฎระเบียบ ซึ่งเป็นบทลงโทษที่รุนแรงและอาจไม่ได้สัดส่วนกับความผิด โดยคณะกรรมการผู้เชี่ยวชาญสามารถออกคำสั่งให้ (1) ดำเนินการแก้ไข หรือ (2) ห้ามกระทำการหรือให้กระทำการเพื่อระงับความเสียหายแก่เจ้าของข้อมูล ทั้งนี้ ถึงแม้การมีกลไกที่จะช่วยส่งเสริมให้มีการปฏิบัติที่ถูกต้องตามกฎระเบียบนับเป็นเรื่องที่สำคัญยิ่ง แต่บีเอสเอยังคงมีความกังวลว่าบทลงโทษของการไม่ปฏิบัติตามกฎระเบียบตามที่เสนอนั้นรุนแรงเกินไปและอาจนำไปสู่การนำข้อกำหนดนี้ไปใช้ในทางที่ผิดได้ ในขณะที่**มาตรา 88** ให้อำนาจแก่เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลไว้อย่างกว้าง โดยสามารถสั่งลงโทษปรับได้ แต่มาตราดังกล่าวกลับไม่ได้ให้แนวทางว่ามีองค์ประกอบในเรื่องใดบ้างที่ควรต้องพิจารณาและมีเหตุบรรเทาโทษใดบ้าง

จากการที่พระราชบัญญัติฉบับนี้ให้แนวทางการปฏิบัติงานแก่คณะกรรมการ สำนักงาน และคณะกรรมการผู้เชี่ยวชาญไว้อย่างจำกัด อีกทั้งยังไม่มีบทบัญญัติที่ชัดเจนเพื่อให้มั่นใจได้ว่าจะมีระบบตรวจสอบและถ่วงดุลอำนาจอย่างเหมาะสมและมีกระบวนการที่ชอบด้วยกฎหมาย บีเอสเอจึงมีความกังวลว่าคณะกรรมการสำนักงาน และคณะกรรมการผู้เชี่ยวชาญอาจออกคำสั่งที่กว้างเกินไป หรือใช้บทลงโทษที่รุนแรงเกินไป จนอาจส่งผลกระทบอย่างร้ายแรงต่อผู้ควบคุมข้อมูล พนักงานของผู้ควบคุมข้อมูล และ/หรือผู้รับจ้างของผู้ควบคุมข้อมูลได้

นอกจากนี้ นับเป็นเรื่องที่สำคัญยิ่งที่มาตรการ แนวทาง หรือกฎระเบียบใดๆ ที่คณะกรรมการจะนำมาใช้ผ่านการใช้อำนาจดังกล่าว ควรจะต้องมีความสอดคล้องกับวิธีปฏิบัติที่ดีและกรอบมาตรฐานที่สากลยอมรับเท่าที่จะเป็นไปได้ ด้วยสภาพเศรษฐกิจดิจิทัลในทั่วโลก จึงมีความจำเป็นอย่างยิ่งที่รัฐบาลต้องไม่กำหนดกฎระเบียบที่ใช้เฉพาะในประเทศในประการที่จะเป็นการขัดขวางการลงทุนในการพัฒนาและใช้เทคโนโลยีที่ทันสมัย ซึ่งไม่ก่อให้เกิดผลประโยชน์แต่ประการใด อีกทั้งยังอาจส่งผลเสียหายต่อความประสงค์ที่มุ่งคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลได้ในหลายกรณี

การมีระบบตรวจสอบและถ่วงดุลอำนาจที่เหมาะสมจะทำให้มั่นใจได้ว่าจะมีความเป็นไปได้ในทางปฏิบัติในเชิงพาณิชย์ที่องค์กรต่างๆ จะสามารถปฏิบัติตามข้อร้องขอให้ส่งเอกสารหรือข้อมูลตลอดจนการสอบสวนได้ นอกจากนี้ ควรมีช่องทางที่เหมาะสมและชัดเจนสำหรับองค์กรต่างๆ ให้สามารถขอให้มีการทบทวนคำสั่งให้เปิดเผยเอกสาร รวมถึงช่องทางในการอุทธรณ์คำสั่งที่ไม่มีเหตุผลอันสมควร อย่างเช่นกรอบและวิธีปฏิบัติในการใช้อำนาจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามบัญชีแนบท้าย 9 แห่งกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ เป็นต้น

ข้อเสนอแนะ

บีเอสเอขอเรียนเสนอว่า ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยควรมีมาตรการป้องกันเพื่อให้การใช้อำนาจรัฐเป็นไปอย่างเหมาะสม โดยสอดคล้องกับหลักการตรวจสอบและถ่วงดุล และกระบวนการที่ชอบด้วยกฎหมาย รวมถึงใน**มาตรา 16, 70, 73 และ 88** โดยไม่กระทบต่อการคุ้มครองประโยชน์โดยชอบด้วยกฎหมายเกี่ยวกับข้อมูลส่วนบุคคล

มาตรการป้องกันที่สามารถกระทำได้ เช่น การกำหนดหลักเกณฑ์อย่างจำกัดและมีความเข้มงวดสำหรับกรณีที่สามารถใช้อำนาจได้ โดยร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรมีช่องทางให้ผู้ควบคุมข้อมูลตลอดจนพนักงานและผู้รับจ้างของผู้ควบคุมข้อมูล สามารถอุทธรณ์คำวินิจฉัยและคำสั่งได้ และโดยเฉพาะอย่างยิ่ง ควรมีกลไกให้สามารถตรวจสอบความชอบด้วยกฎหมายของคำวินิจฉัยได้ นอกจากนี้ เพื่อให้มีกระบวนการที่เปิดเผยและโปร่งใสในการกำหนดมาตรการหรือวิธีการ และในการออกประกาศ หลักเกณฑ์ หรือแนวทาง จึงเป็นการสมควรที่คณะกรรมการจะขอรับฟังความเห็นจากผู้มีส่วนได้เสียและพิจารณาความเห็นของภาคอุตสาหกรรมด้วย

นอกจากนี้ บีเอสเอขอเรียนเสนอให้เพิ่มหลักเกณฑ์ใน**มาตรา 88** สำหรับวิธีการที่เลขานุการจะกำหนดโทษปรับและโทษอื่นๆ และเหตุบรรเทาโทษ

ความรับผิดทางแพ่งและทางอาญา (มาตรา 75-79)

เอ. ความรับผิดทางแพ่ง

มาตรา 75 เป็นการกำหนดความรับผิดโดยเด็ดขาดโดยไม่พิจารณาถึงกรณีที่กระทำการไปโดยมีเหตุผลอันสมควรหรือเพื่อบรรเทาความเสียหายที่อาจเกิดขึ้น

นอกจากนี้ การชดใช้ความเสียหายตามที่กำหนดไว้ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ไม่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของที่ใดในโลก รวมถึง GDPR ผู้ประมวลผลข้อมูลไม่ควรมีความรับผิดต่อเจ้าของข้อมูล เว้นแต่ในกรณีที่ผู้ประมวลผลข้อมูลกระทำขัดกับคำสั่งอันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล โดยทั่วไปแล้วผู้ประมวลผลข้อมูลจะไม่ต้องตัดสินใจเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมุลส่วนบุคคล และมีข้อมูลเพียงเล็กน้อยหรือไม่มีข้อมูลเลยสำหรับการตัดสินใจในเรื่องเหล่านี้ ด้วยเหตุนี้ ผู้ประมวลผลข้อมูลจึงไม่ควรมีความรับผิดในการชดใช้ความเสียหายเช่นเดียวกับผู้ควบคุมข้อมูล

ข้อเสนอแนะ

นอกเหนือจากการแก้ไขเพิ่มเติมที่เรียนเสนอข้างต้นในข้อ 1(II) ของหนังสือนี้ ที่ได้เสนอให้ตัดส่วนที่กล่าวถึง “ผู้ประมวลผลข้อมูล” ใน**มาตรา 75 และ 76** ออกไปแล้วนั้น บีเอสเอขอเรียนให้แก้ไขเพิ่มเติมบทบัญญัตินี้ให้สอดคล้องกับ GDPR กล่าวคือ ผู้ประมวลผลข้อมูลจะมีความรับผิดต่อความเสียหายที่เกิดจากการประมวลผลข้อมูลเฉพาะในกรณีที่การประมวลผลข้อมูลนั้นไม่เป็นไปตามพระราชบัญญัตินี้

นอกจากนี้ **มาตรา 76** ควรมีหลักเกณฑ์ที่โปร่งใสยิ่งขึ้นในการกำหนดโทษทางปกครอง เช่น โดยการกำหนดให้มีข้อพิจารณาตามข้อ 83 ของ GDPR ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับปัจจุบันให้อำนาจศาลอย่างกว้างขวางโดยไม่มีหลักเกณฑ์ที่ชัดเจนที่จะช่วยเป็นแนวทางในการใช้ดุลพินิจของศาลอย่างยุติธรรมและโปร่งใสแต่อย่างใด

อีกทั้งเป็นการเหมาะสมที่จะกำหนดให้มีปัจจัยเพิ่มเติมที่อาจปกป้องผู้ควบคุมข้อมูลจากความรับผิดโดยเด็ดขาด โดยบีเอสเอขอเรียนเสนอให้แก้ไข**มาตรา 75 และ 76** ดังนี้

> ***มาตรา 75***
>
> *ผู้ควบคุมข้อมูลส่วนบุคคล**~~หรือผู้ประมวลผลข้อมูลส่วนบุคคล~~** ซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคล**~~หรือผู้ประมวลผลข้อมูลส่วนบุคคล~~**นั้นจะพิสูจน์**หรือแสดงให้เห็น**ได้ว่า*
>
> *. . .*

(3) เป็นการกระทำการไปโดยมีเหตุผลอันสมควรหรือเพื่อบรรเทาความเสียหายที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดต่อความเสียหายที่เกิดจากการประมวลผลข้อมูลก็ต่อเมื่อผู้ประมวลผลข้อมูลส่วนบุคคลไม่ได้ปฏิบัติหน้าที่ของตนตามพระราชบัญญัตินี้

มาตรา 76

*ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคล~~**หรือผู้ประมวลผลข้อมูลส่วนบุคคล**~~จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้น. . . ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคล~~**หรือผู้ประมวลผลข้อมูลส่วนบุคคล**~~ได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคล~~**หรือผู้ประมวลผลข้อมูลส่วนบุคคล**~~ การที่ผู้ควบคุมข้อมูลส่วนบุคคล~~**หรือผู้ประมวลผลข้อมูลส่วนบุคคล**~~ได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย*

*สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ . . .รู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล~~**หรือผู้ประมวลผลข้อมูลส่วนบุคคล**~~ที่ต้องรับผิด. . .*

บี. ความรับผิดทางอาญา

บีเอสเอมีความกังวลอย่างยิ่งที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีบทกำหนดโทษอาญา รวมถึงความรับผิดอาญาของบุคคลธรรมดา สำหรับการกระทำที่ขัดต่อกฎหมายนี้ สำหรับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแล้ว โทษอาญาไม่ได้มีบทบาทที่เป็นประโยชน์แต่อย่างใด แม้ในบางประเทศจะมีการกำหนดโทษอาญาเช่นกัน แต่ก็ไม่ใช่ทางปฏิบัติของสากล ทางแก้ไขเยียวยาดังกล่าวจึงเกินสัดส่วนกับความเสี่ยงที่กล่าวไว้ในกรอบกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อกำหนดส่วนที่เป็นกฎหมายสารบัญญัติในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ตลอดจนค่าสินไหมทดแทนที่เป็นตัวเงินและทางแก้ไขเยียวยาเพื่อควบคุมการกระทำ ผ่านทางกระบวนการทางปกครองหรือทางแพ่งนั้นก็เป็นการเพียงพอแล้วสำหรับการคุ้มครองความเป็นส่วนตัวของบุคคล ในทางตรงข้าม ความเสี่ยงว่าจะมีความรับผิดทางอาญาอาจทำให้บริษัทต่างๆ ไม่กล้าดำเนินการเกี่ยวกับข้อมูลแม้จะเป็นการดำเนินการที่มีประโยชน์และไม่ก่อให้เกิดความเสียหายก็ตาม ดังที่เรียนไว้ในส่วนถัดไปในหนังสือนี้ นอกจากนี้ ความรับผิดทางอาญาตามกฎหมายนี้มีมาตรฐานต่ำเกินควร โดยใน**มาตรา 77 วรรคหนึ่ง** ได้กำหนดโทษอาญาสำหรับการไม่ปฏิบัติตามบทบัญญัติในพระราชบัญญัตินี้ตามมาตราที่ระบุไว้เพียงแค่โดยประการที่*น่าจะ*ทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง เป็นต้น

นอกจากนี้ ร่างพระราชบัญญัตินี้มีบทกำหนดโทษอาญาแก่บุคคลธรรมดาใน**มาตรา 78** สำหรับ “*ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น*” และ

ใน**มาตรา 79** ในกรณีที่ "*ผู้กระทำความผิดตามพระราชบัญญัตินี้. . . ถ้าการกระทำความผิด . . . นั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใด. . .ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สาหรับความผิดนั้น ๆ ด้วย*" ซึ่งเป็นบทบัญญัติที่น่ากังวลเป็นอย่างยิ่ง

การกำหนดให้ "บุคคลใด" มีความรับผิดเป็นเรื่องที่ไม่เหมาะสมเมื่อพิจารณาถึงลักษณะของการปฏิบัติในการคุ้มครองข้อมูลและจัดการข้อมูล ตัวอย่างเช่น การกระทำความผิดเกี่ยวกับการไม่ปฏิบัติหน้าที่ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่ไม่เข้าข้อยกเว้นตาม**มาตรา 24** นั้น บุคคลที่อาจเกี่ยวข้องกับการไม่ปฏิบัติหน้าที่ดังกล่าวอาจมีจำนวนมากมาย ซึ่งมีหน้าที่ความรับผิดชอบที่หลากหลายและอาจอยู่ในหลายประเทศ ซึ่งบทบัญญัตินี้จะทำให้บุคคลมากมายที่มีหน้าที่ความรับผิดชอบเพียงเล็กน้อยจะต้องมีความผิดไปด้วย ด้วยเหตุนี้ ผู้ที่ควรมีความรับผิดสำหรับการกระทำความผิดนี้จึงได้แก่บริษัท ไม่ใช่บุคคลธรรมดา ค่าปรับที่มีจำนวนสูงที่กำหนดต่อบริษัท และความเสี่ยงอื่นๆ จากการไม่ปฏิบัติตามกฎหมาย เช่น เสียชื่อเสียงและธุรกิจได้รับผลกระทบ ก็เป็นการเพียงพอแล้วที่จะทำให้บริษัทต่างๆ ห้ามพนักงานของตนมิให้ละเมิดนโยบายต่างๆ ที่บริษัทต้องมีเพื่อให้แน่ใจได้ว่ามีการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ข้อเสนอแนะ

ด้วยเหตุนี้ บีเอสเอเห็นเป็นเรื่องจำเป็นที่จะต้องตัดบทบัญญัติที่กำหนดความรับผิดทางอาญาสำหรับการกระทำที่ขัดต่อร่างพระราชบัญญัติฉบับนี้**โดยการตัดมาตรา 77-79 ออกไปทั้งมาตรา**

ขอบเขตพื้นที่ที่บังคับใช้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (มาตรา 5)

มาตรา 5 ของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการแก้ไขให้ครอบคลุมถึงการกระทำของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่อยู่ "*นอกราชอาณาจักร*" ด้วย สำหรับกิจกรรมที่เกี่ยวข้องกับ "*การเสนอสินค้าหรือบริการ*" และ "*การเฝ้าติดตามพฤติกรรม*" ของเจ้าของข้อมูลที่อยู่ในราชอาณาจักร บีเอสเอเห็นว่าควรจำกัดขอบเขตของร่างพระราชบัญญัตินี้ไว้เพียงนิติบุคคลหรือกิจกรรมที่มีความเกี่ยวข้องใกล้ชิดอย่างเพียงพอกับประเทศไทยเพื่อให้แน่ใจว่าจะสามารถบังคับตามคำสั่งต่อนิติบุคคลต่างประเทศได้อย่างมีประสิทธิภาพ

บีเอสเอขอเรียนเสนอให้จำกัดขอบเขตการบังคับใช้กฎหมายการคุ้มครองข้อมูลส่วนบุคคลนี้ไว้เพียงการประมวลผลข้อมูลที่กระทำโดยบุคคลธรรมดาหรือนิติบุคคล ไม่ว่าเป็นหน่วยงานภาครัฐหรือเอกชน โดยมีเงื่อนไขว่า (1) การกระทำนั้นมุ่งเป้าไปที่ผู้ที่อยู่ในประเทศไทยโดยเฉพาะ (2) ข้อมูลส่วนบุคคลที่ประมวลผลนั้นจงใจเก็บรวบรวมมาจากเจ้าของข้อมูลที่อยู่ในประเทศไทยในขณะที่มีการเก็บรวบรวม และ (3) การเก็บรวบรวมนั้นกระทำโดยนิติบุคคลที่จัดตั้งขึ้นในประเทศไทยและมีความพร้อมที่จะดำเนินการในเรื่องนี้เพื่อให้สามารถดำเนินกิจกรรมได้อย่างแท้จริงและมีประสิทธิภาพ หรือนิติบุคคลที่ต้องปฏิบัติตามกฎหมายไทยโดยอาศัยกฎหมายมหาชนระหว่างประเทศ โดยมาตรฐานนี้ การที่สามารถเข้าเว็บไซต์หนึ่งๆ ได้ในประเทศไทยหรือการใช้ภาษาไทยเพียงเท่านั้นจึงไม่เพียงพอที่จะนำไปสู่การบังคับใช้พระราชบัญญัตินี้

บทเฉพาะกาล (มาตรา 2)

เป็นเรื่องสำคัญยิ่งที่พระราชบัญญัตินี้ต้องไม่มีผลย้อนหลังและต้องให้ระยะเวลาตามสมควรระหว่างวันที่ตรากฎหมายขึ้นกับวันที่มีผลบังคับใช้ บุคคลธรรมดา ธุรกิจ และรัฐบาลจะได้รับประโยชน์จากช่วงเปลี่ยนผ่านที่เป็น

ระบบซึ่งไม่ทำให้เกิดการเปลี่ยนแปลงอย่างฉับพลันต่อการปฏิบัติและความเสี่ยง อีกทั้งไม่ทำให้องค์กรต้องเร่งปรับใช้การเปลี่ยนแปลงนั้นในทางปฏิบัติเนื่องจากเกรงว่าจะได้รับโทษ ในร่างพระราชบัญญัติฉบับปัจจุบัน **มาตรา 2** ระบุว่ากฎหมายนี้จะใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป ซึ่งระยะเวลาหนึ่งร้อยแปดสิบวันนั้นเป็นระยะเวลาที่สั้นเป็นอย่างยิ่งและไม่เพียงพอให้องค์กรต่างๆ ปฏิบัติตามข้อกำหนดของพระราชบัญญัตินี้ได้ นอกจากนี้ยังไม่สอดคล้องกับวิธีปฏิบัติของสากลอีกด้วย โดยในประเทศหรือเขตปกครองอื่นๆ จะกำหนดช่วงเปลี่ยนผ่านไว้ที่สองปี ด้วยเหตุนี้ **บีเอสเอจึงขอเรียนเสนอให้มาตรา 2 กำหนดระยะเวลาเป็น *ไม่น้อยกว่าสองปี***

บทสรุป

บีเอสเอขอแสดงความชื่นชมที่สภานิติบัญญัติจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความทันสมัยเพื่อคุ้มครองความเป็นส่วนตัวของพลเมืองไทย การร่างกฎหมายอย่างเหมาะสมจะสามารถนำไปสู่การบังคับสิทธิอย่างมีประสิทธิภาพได้ ด้วยเหตุนี้ บีเอสเอจึงขอให้ท่านได้โปรดพิจารณาความเห็นและข้อเสนอแนะข้างต้นอย่างถี่ถ้วนเพื่อให้เกิดประโยชน์สูงสุดแก่ทุกฝ่าย

บีเอสเอยินดีจะหารือกับท่านหรือผู้แทนของท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่** varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591**

บีเอสเอขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้