สำนักงานคณะกรรมการกฤษฎีกา
เลขที่ ๑ ถนนพระอาทิตย์
เขตพระนคร กรุงเทพฯ ๑๐๒๐๐

วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๕๗

สำคัญและเป็นความลับ

เรื่อง ข้อคิดเห็นและข้อเสนอแนะเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (ฉบับล่าสุด)

เรียน เลขาธิการคณะกรรมการกฤษฎีกา

กลุ่มพันธมิตรธุรกิจซอฟต์แวร์ หรือ บีเอสเอ (BSA)[1] รู้สึกยินดีเป็นอย่างยิ่งที่ได้รับโอกาสให้แสดงข้อคิดเห็นและข้อเสนอแนะเกี่ยวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (ฉบับล่าสุด) ทั้งนี้บีเอสเอได้ติดตามดูพัฒนาการของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาอย่างใกล้ชิด และใคร่ขอขอบคุณสำหรับวิธีการที่โปร่งใสที่ใช้ในการหารือ และแสดงทัศนะเกี่ยวกับร่างพระราชบัญญัติฉบับดังกล่าว

[1] กลุ่มพันธมิตรธุรกิจซอฟต์แวร์ หรือ บีเอสเอ (www.bsa.org) เป็นตัวแทนให้กับอุตสาหกรรมซอฟต์แวร์ทั่วโลกในการติดต่อกับรัฐบาล หรือในตลาดทั่วโลก สมาชิกของบีเอสเอเป็นบริษัทที่มีนวัตกรรมล้ำหน้ามากที่สุดหลายบริษัทของโลก ซึ่งได้สร้างระบบซอฟต์แวร์ที่กระตุ้นเศรษฐกิจ และปรับปรุงชีวิตสมัยใหม่ให้ดีขึ้น บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดีซี และมีการดำเนินงานอยู่ในประเทศต่างๆ มากกว่า ๖๐ ประเทศทั่วโลก โดยบีเอสเอเป็นผู้นำในเรื่องแผนงานในการตรวจสอบและกำกับดูแลการปฏิบัติงานซึ่งสนับสนุนการใช้ซอฟต์แวร์อย่างถูกกฎหมาย และให้ความสนับสนุนเกี่ยวกับนโยบายสาธารณะที่สร้างเสริมนวัตกรรมด้านเทคโนโลยี และผลักดันความเจริญเติบโตของเศรษฐกิจดิจิตอล (Digital Economy) สมาชิกของบีเอสเอมีมากมายหลายบริษัทซึ่งรวมทั้ง Adobe, Agilent Technologies, ANSYS, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IMB, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, Siemens PLM, Symantec, Tekla และ The MathWorks

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

สมาชิกของบีเอสเอตระหนักดีถึงความสำคัญในการสร้างความเชื่อมั่นและความมั่นใจในพื้นที่ออนไลน์ และด้วยเหตุนี้จึงมีเจตนาแน่วแน่ที่จะคุ้มครองข้อมูลส่วนบุคคล ทั้งในด้านเทคโนโลยีและรูปแบบธุรกิจประเภทต่างๆ สมาชิกของบีเอสเอเป็นบริษัทแถวหน้าในการสร้างสรรค์นวัตกรรมด้านข้อมูล รวมทั้งการพัฒนาเทคโนโลยีแบบ Cloud-based ซึ่งช่วยส่งเสริมการพัฒนาทางเศรษฐกิจ และประสิทธิภาพโดยการทำให้บุคคลทั่วไป และธุรกิจขนาดเล็กสามารถเพิ่มกำลังความสามารถด้านคอมพิวเตอร์ ซึ่งครั้งหนึ่งไม่สามารถทำได้เนื่องจากติดปัญหาเรื่องค่าใช้จ่าย

การพัฒนาเทคโนโลยีเหล่านี้อย่างต่อเนื่องจำเป็นต้องมีกรอบกฎหมายซึ่งกำหนดไว้อย่างชัดเจน และมีความยืดหยุ่นตามสมควร กฎหมายคุ้มครองข้อมูลจะต้องคุ้มครองความเป็นส่วนตัวของผู้บริโภคโดยไม่สร้างอุปสรรคที่ไม่จำเป็นอันเป็นการกีดกันการไหลเวียนของข้อมูลอย่างอิสระ ซึ่งเป็นสิ่งสำคัญอย่างยิ่งสำหรับเศรษฐกิจในศตวรรษที่ 21 นี้ แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลซึ่งปัจจุบันอยู่ในระหว่างการพิจารณาของคณะกรรมการกฤษฎีกาจะได้รับการปรับปรุงให้ดีขึ้นกว่าฉบับก่อนหน้านี้เป็นอย่างมาก แต่บีเอสเอขอแสดงข้อคิดเห็นเพื่อชี้ให้เห็นถึงบทบัญญัติหลายๆ บทซึ่งอาจก่อให้เกิดภาระอันไม่จำเป็นและความไม่แน่นอนด้านกฎหมายแก่ภาคส่วนเทคโนโลยี

มาตรา 5: นิยามศัพท์

"ข้อมูลส่วนบุคคล" – คำนิยามที่เสนอตั้งอยู่บนแนวคิดในเรื่องข้อมูลส่วนบุคคลที่ใช้ในกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) และกฎหมายว่าด้วยการคุ้มครองข้อมูลของสหภาพยุโรป (European Data Protection Directive) ซึ่งใช้กับข้อมูลทุกประเภท โดยไม่คำนึงถึงรูปแบบหรือเนื้อหา ไม่ว่าข้อมูลนั้นทำให้สามารถระบุตัวบุคคลนั้นได้หรืออาจทำให้สามารถระบุตัวบุคคลนั้นได้ อย่างไรก็ตามคำนิยามที่มีความหมายกว้างดังกล่าวได้กลายเป็นประเด็นที่มีการแสดงความคิดเห็นกันอย่างมากในสหภาพยุโรป ตัวอย่างเช่นในกรณีที่ไม่มีการทำวิจัยทางการแพทย์ในบางเรื่องในสหภาพยุโรปอย่างที่ได้คาดการณ์ไว้ เนื่องจากมีข้อกำหนดที่เข้มงวดในเรื่องต้องได้รับความยินยอมล่วงหน้าถึงแม้ว่าข้อมูลนั้นไม่สามารถระบุตัวบุคคลที่เกี่ยวข้อง (Data Subjects) ได้โดยตรงจากข้อมูลที่จัดให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลก็ตาม การนำภาระหน้าที่ทางกฎหมายที่เข้มงวดอย่างมากมาใช้บังคับกับข้อมูลในวงกว้างโดยไม่คำนึงถึงบริบทของข้อมูล และความเป็นไปได้ว่าจะก่อให้เกิดอันตรายกับตัวบุคคลที่เกี่ยวข้องกับข้อมูลนั้นจริงหรือไม่ อาจเป็นตัวทำลายการเจริญเติบโตทางเศรษฐกิจของประเทศไทยโดยขัดขวางความคิดริเริ่มหรือนวัตกรรมใหม่ๆ ที่ใช้ประโยชน์จากข้อมูล

เพื่อหลีกเลี่ยงกรณีดังกล่าว บีเอสเอใคร่ขอเสนอให้คณะกรรมการกฤษฎีกานำแนวคิดในเรื่องข้อมูลส่วนบุคคลมาใช้โดยดูจากบริบท ซึ่งตามแนวคิดดังกล่าวข้อมูลจะถือเป็น "ข้อมูลส่วนบุคคล" เฉพาะใน

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถระบุตัวบุคคลที่เกี่ยวข้องกับข้อมูลดังกล่าวได้เท่านั้น ดังนั้น บีเอสเอใคร่ขอเสนอให้มีการแก้ไขคำนิยามเป็นดังนี้

> *"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม*

"ผู้ควบคุมข้อมูลส่วนบุคคล" - สอดคล้องกับกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) คำนิยามที่เสนอของคำว่า "ผู้ควบคุมข้อมูลส่วนบุคคล" รับรองว่าบุคคลหรือองค์กรนิติบุคคลซึ่งมีอำนาจในการตัดสินใจเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลจะอยู่ในฐานะที่ดีที่สุดในการกำกับดูแลความสมบูรณ์ของข้อมูลดังกล่าว และเพื่อให้สอดคล้องกับกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกายืนยันว่าบทบัญญัติดังกล่าวไม่เกี่ยวโยงกับผู้ให้บริการประเภท Cloud Services ซึ่งอาจเป็นผู้จัดหาฮาร์ดแวร์ และ/หรือ ซอฟต์แวร์ บนเครือข่ายคอมพิวเตอร์ (Host) หรือประมวลผลเกี่ยวกับข้อมูลตามคำสั่งของผู้ใช้บริการ บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาเพิ่มเติมข้อความต่อไปนี้ซึ่งเป็นข้อความที่อยู่ในกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) ไว้ในคำนิยามดังกล่าวด้วย

> *"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า ผู้ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งรวมถึงการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ แต่ไม่รวมบุคคล หรือองค์กรซึ่งปฏิบัติงานดังกล่าวตามที่ได้รับคำสั่งจากบุคคล หรือองค์กรอีกแห่งหนึ่ง หรือโดยหน้าที่ตามสัญญา หรือหน้าที่ตามกฎหมาย*

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 7 - มาตรา 18)

บีเอสเอให้การสนับสนุนอย่างเต็มที่สำหรับความพยายามของประเทศไทยที่จะตั้งคณะบุคคลที่มีหน้าที่รับผิดชอบอย่างเป็นทางการเรื่องการคุ้มครองข้อมูลส่วนบุคคลแบบรวมศูนย์ คณะบุคคลดังกล่าวสามารถมีบทบาทสำคัญในการให้ความรู้แก่ผู้บริโภคเกี่ยวกับการเลือกวิธีการเก็บรวบรวม ใช้ และจัดเก็บข้อมูลส่วนบุคคลของตน ผู้ใช้คอมพิวเตอร์ทั้งที่เป็นผู้บริโภคและธุรกิจต่างๆ ควรได้รับความรู้เกี่ยวกับวิธีป้องกันตนเองจากความเสี่ยงต่างๆ ที่เพิ่มมากขึ้นเรื่อยๆ ในโลกออนไลน์ ซึ่งรวมทั้งการหลอกลวง และการโจรกรรมเอกลักษณ์บุคคล ทั้งนี้การคุ้มครองความเป็นส่วนตัวขึ้นอยู่กับผู้บริโภคที่ได้รับข้อมูลที่ครบถ้วนสมบูรณ์ ธุรกิจที่มีความรับผิดชอบ และการบังคับใช้กฎหมายด้วยความระมัดระวังรอบคอบ แนวทาง "การรับผิดชอบร่วมกัน" ในเรื่องการคุ้มครองความเป็นส่วนตัวทำให้

ผู้บริโภคจะต้องตระหนักถึงวิธีปฏิบัติเกี่ยวกับการคุ้มครองความเป็นส่วนตัว สามารถตัดสินใจเลือกว่าจะให้ใช้ข้อมูลส่วนบุคคลของตนอย่างไร และจะต้องปกป้องข้อมูลภายใต้การควบคุมของตน

นอกจากนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังสามารถมีบทบาทสำคัญในการกำกับดูแลการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งในเรื่องดังกล่าว บีเอสเอมีความกังวลว่าบทบัญญัติหลายบทอาจเป็นการมอบหมายอำนาจซึ่งกว้างเกินไป ยกตัวอย่างเช่นบีเอสเอเห็นว่ามาตรา 13 (4) และมาตรา 13 (11) ดูเหมือนจะให้อำนาจคณะกรรมการในการเข้าแทรกแซงวิธีปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบริษัท แม้จะไม่มีหลักฐานที่แสดงว่าบริษัทดังกล่าวไม่ได้ปฏิบัติตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก็ตาม และมาตรา 16 ได้ให้คณะกรรมการมีอำนาจเรียกตัวมาชี้แจงข้อเท็จจริง ไม่ใช่เฉพาะในกรณีไต่สวนข้อร้องเรียนเท่านั้น แต่ยังรวมไปถึง "เรื่องอื่นๆ " ที่คณะกรรมการเห็นว่าเหมาะสมอีกด้วย การมอบหมายอำนาจให้โดยไม่มีขอบเขตจำกัดนี้เป็นเรื่องที่สร้างความกังวล อย่างน้อยเพื่อเป็นไปตามกระบวนการยุติธรรมอันควรตามกฎหมาย บีเอสเอเห็นว่าเป็นเรื่องสำคัญที่อำนาจต่างๆ ตามมาตรา 13 (4) มาตรา 13 (11) และมาตรา 16 ควรจะมีขอบเขตจำกัดเฉพาะ โดยให้เป็นเฉพาะในกรณีที่คณะกรรมการมีความสงสัยโดยมีเหตุผลตามสมควรว่าผู้ควบคุมข้อมูลส่วนบุคคลได้กระทำการฝ่าฝืนบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

อำนาจของคณะกรรมการในการออก "มาตรการหรือแนวทาง" เกี่ยวกับวิธีปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลตามมาตรา 13 (3) ควรได้รับการจำกัดให้แคบลงด้วยเช่นกัน และควรมีการกำกับให้คณะกรรมการดำเนินการดูแลให้มาตรการที่ออกมามีความเป็นกลางทางเทคโนโลยี และไม่ควรมีการกำหนดแนวทางในลักษณะ "วิธีการแบบเดียวซึ่งใช้กับทุกกรณี" (one-size-fits-all) เพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล นอกจากนี้แนวทางปฏิบัติที่ออกโดยคณะกรรมการต้องไม่ผิดต่างไปจากมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไปว่าด้วยเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งในเรื่องนี้ ควรให้อำนาจแก่คณะกรรมการสำหรับออกแนวทางเฉพาะเท่าที่สอดคล้องกับมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลที่เป็นที่ยอมรับทั่วโลก ได้แก่ ISO/IEC 27001:2005 และ ISO/IEC 17799:2005 หลักการดังกล่าวควรต้องนำเข้ามารวมไว้ในมาตรา 33 ถึงมาตรา 35 ซึ่งให้อำนาจคณะกรรมการในการกำหนดประมวลหลักปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้วย

การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 21 ถึง มาตรา 25)

มาตรา 21 ถึงมาตรา 25 สร้างกรอบการดำเนินการโดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้ทราบเกี่ยวกับลักษณะของการเก็บรวบรวมข้อมูล บีเอสเอเห็นด้วยว่าข้อกำหนดให้ทำการแจ้งให้เจ้าของ

ข้อมูลส่วนบุคคลทราบก่อน หรือในเวลาที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล เป็นเรื่องที่สมเหตุสมผล ตามปกติสมาชิกของบีเอสเอจะทำการแจ้งให้ทราบผ่านการใช้นโยบายคุ้มครองความเป็นส่วนตัวที่เข้าถึงได้ง่าย ซึ่งจะให้ข้อมูลโดยละเอียดแก่ผู้ใช้บริการเกี่ยวกับขอบเขตของข้อมูลที่จะเก็บรวบรวม และวัตถุประสงค์ในการเก็บรวบรวม

ดังที่มาตรา 23 ของร่าง พรบ. รับรอง มีหลายกรณีที่การแจ้งให้ผู้ใช้บริการทราบก่อนทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอาจไม่สมเหตุสมผลหรือไม่เหมาะสม นอกเหนือจากกรณีที่แจกแจงไว้ในมาตรา 23 (1 - 6) แล้ว การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลบางอย่างอาจจำเป็นในการดำเนินกิจกรรมทางธุรกิจตามปกติและชอบด้วยกฎหมาย บีเอสเอจึงใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณานำข้อยกเว้นเพิ่มเติมมารวมไว้ในมาตรา 23 เพื่อช่วยให้การเก็บรวบรวมข้อมูลเป็นไปโดยสะดวกเพื่อประโยชน์ในการดำเนินการให้เป็นไปตาม "ประโยชน์อันชอบด้วยกฎหมาย" (Legitimate Interests) ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งข้อยกเว้นดังกล่าวสอดคล้องกับแนวทางในการคุ้มครองความเป็นส่วนตัวในกฎหมายว่าด้วยการคุ้มครองข้อมูลของสหภาพยุโรป (95/46/อีซี) ข้อยกเว้นดังกล่าวนอกจากจะมีความสำคัญที่ทำให้การดำเนินกิจกรรมทางธุรกิจตามสมควรเกี่ยวกับข้อมูลส่วนบุคคลไม่มีภาระหรือไม่ล่าช้าเกินควร (เช่น การประมวลผลความมั่นคงปลอดภัยของข้อมูลและเครือข่าย) แล้ว ยังส่งเสริมการคุ้มครองข้อมูลและการลดการเก็บรวบรวมข้อมูล (Data Minimization) โดยลดมูลเหตุจูงใจต่างๆ ที่นำไปสู่การเก็บข้อมูลส่วนบุคคลที่มากเกินจำเป็น การไม่มีข้อยกเว้นในเรื่อง "ประโยชน์อันชอบด้วยกฎหมาย" (Legitimate Interests) นั้น อาจทำให้ร่าง พรบ. กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บข้อมูลมากกว่าที่จำเป็นเพื่อวัตถุประสงค์ทางธุรกิจของตน เพียงเพื่อจะปฏิบัติตามข้อกำหนดในการแจ้งให้ทราบเรื่องการเก็บข้อมูลเท่านั้น การมีข้อยกเว้นในเรื่อง "ประโยชน์อันชอบด้วยกฎหมาย" (Legitimate Interests) จึงช่วยส่งเสริมการลดการเก็บรวบรวมข้อมูล (Data Minimization) โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมเฉพาะข้อมูลที่เกี่ยวข้องกับความต้องการบางอย่างของตนเท่านั้น บีเอสเอจึงใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณาเพิ่มข้อยกเว้นต่อไปนี้ในมาตรา 23

(7) ข้อมูลที่เก็บรวบรวมเพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 24 ก่อให้เกิดประเด็นในลักษณะเดียวกัน โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเก็บรวบรวมข้อมูลจากแหล่งข้อมูลที่เป็นบุคคลภายนอก จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นเจ้าของข้อมูลที่เกี่ยวโยงกับการดำเนินการนั้นทราบโดยทันที อย่างไรก็ตามอาจมีกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะได้รับข้อมูลส่วนบุคคลบางอย่างมา แต่ขาดข้อมูลที่จำเป็นบางอย่างที่จะทำให้สามารถแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบตามที่กำหนดไว้ได้ เพื่อหลีกเลี่ยงสถานการณ์ที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องให้ได้มาซึ่งข้อมูลสำหรับติดต่อเป็นการส่วนตัวของผู้ใช้บริการแต่ละรายซึ่ง

ข้อมูลของพวกเขาถูกรวมอยู่ในการโอนข้อมูลจากแหล่งข้อมูลที่เป็นบุคคลภายนอก บีเอสเอจึงใคร่ขอเสนอให้คณะกรรมการกฤษฎีกาพิจารณาแก้ไขมาตรา 24 เป็นดังนี้

> *เมื่อทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลอื่นนอกเหนือจากเก็บจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบทันทีเกี่ยวกับการเก็บรวบรวมดังกล่าว ทั้งนี้ เท่าที่สามารถดำเนินการได้*
>
> *การแจ้งให้ทราบตามวรรค 1 ไม่จำต้องดำเนินการ หากข้อมูลได้รับการเก็บรวบรวมตามข้อยกเว้นในมาตรา 23*

มาตรา 25 ห้ามมิให้เก็บรวบรวมข้อมูลที่อ่อนไหว (Sensitive Data) โดยปราศจากความยินยอม ถึงแม้ว่าเป็นเรื่องเหมาะสมในบางกรณีที่จะมีข้อกำหนดที่เข้มงวดมากขึ้นสำหรับการเก็บรวบรวมและใช้ข้อมูลที่อ่อนไหวบางอย่าง แต่ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีความเข้าใจที่ชัดเจนว่าเมื่อใดที่ต้องปฏิบัติตามข้อกำหนดที่เข้มงวดดังกล่าวนั้น ในเรื่องนี้บีเอสเอมีความกังวลว่าข้อบังคับที่ว่าจะต้องได้รับความยินยอมก่อนจึงจะสามารถทำการเก็บรวบรวม "ข้อมูลซึ่งกระทบความรู้สึกของผู้อื่นหรือประชาชน" ได้ จะก่อให้เกิดความไม่ชัดเจนเป็นอย่างมากสำหรับผู้ควบคุมข้อมูลส่วนบุคคล การที่ข้อมูลส่วนบุคคลจะ "กระทบความรู้สึก" ของเจ้าของข้อมูลส่วนบุคคลหรือไม่นั้นเป็นการตัดสินที่มาจากความเชื่อและความรู้สึกส่วนบุคคลสูงมาก โดยไม่ได้มาจากข้อเท็จจริง บุคคลสองคนอาจมีปฏิกิริยาโต้ตอบที่แตกต่างกันอย่างสิ้นเชิงเมื่อทราบเกี่ยวกับการเก็บรวบรวมข้อมูลบางอย่าง ดังนั้นจึงเป็นไปไม่ได้สำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่จะรู้ว่าเมื่อใดที่ตนจะมีภาระหน้าที่ตามมาตรา 25 บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณานำข้อความนี้ออกจากมาตรา 25 นอกจากนี้เพื่อให้สอดคล้องกับมาตรา 23 (4) ใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณาขยายข้อยกเว้นสำหรับมาตรา 25 เพื่อที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลที่ได้ถูก "เปิดเผยต่อสาธารณะโดยชอบด้วยกฎหมาย" อยู่แล้วได้อย่างอิสระ และเพื่อจะบรรลุวัตถุประสงค์ดังกล่าว บีเอสเอใคร่ขอเสนอให้มีการแก้ไขข้อความเป็นดังนี้

> *ห้ามมิให้เก็บรวบข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม <u>หรือ</u> ข้อมูลสุขภาพ ~~หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของผู้อื่นหรือประชาชน~~ตามที่คณะกรรมการประกาศกำหนด โดยปราศจากความยินยอมจากเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง เว้นแต่*
>
> 1. *ได้รับการยกเว้นตามมาตรา 23 (2) (3) <u>(4)</u> หรือ (5)*
> 2. *กรณีอื่นตามที่กำหนดในกฎกระทรวง*

การใช้ข้อมูลส่วนบุคคล (มาตรา 26)

บีเอสเอยังมีความกังวลเป็นอย่างยิ่งว่าร่าง พรบ. ดังกล่าวอาจได้รับการตีความให้มีการกำหนดหน้าที่แยกต่างหากสำหรับผู้ควบคุมข้อมูลส่วนบุคคล โดยกำหนดให้ขอความยินยอมก่อนที่จะใช้ข้อมูลที่ได้มาโดยชอบด้วยกฎหมายซึ่งเจ้าของข้อมูลส่วนบุคคลเองได้รับทราบแล้ว นอกจากภาระหน้าที่ในมาตรา 22 ที่จะต้องแจ้งให้ผู้บริโภคทราบเกี่ยวกับการ *เก็บรวบรวม* ข้อมูลส่วนบุคคลแล้ว มาตรา 26 อาจถูกตีความให้ผู้ควบคุมข้อมูลมีหน้าที่แยกต่างหาก โดยต้องขอรับความยินยอมก่อนการใช้ข้อมูลดังกล่าว ซึ่งบทบัญญัติดังกล่าวขัดแย้งกับกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) และในทางปฏิบัติแล้ว ไม่สามารถทำได้ในสภาพแวดล้อมที่เป็นระบบคลาวด์คอมพิวติ้ง (Cloud) สมัยใหม่

กรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) ได้กำหนดระบบที่สมเหตุสมผลที่ทำให้แน่ใจได้ว่าผู้บริโภคได้รับแจ้งให้ทราบเกี่ยวกับประเภทของข้อมูล ที่ผลิตภัณฑ์หรือบริการออนไลน์จะเก็บรวบรวม และวิธีใช้ข้อมูลดังกล่าว ในการปฏิบัติตาม "หลักการแจ้งให้ทราบ" นั้น โดยทั่วไปผู้ให้บริการทางออนไลน์จะคงไว้ซึ่งนโยบายการคุ้มครองความเป็นส่วนตัวที่ผู้ใช้บริการสามารถศึกษาพิจารณาก่อนที่จะมีการเก็บรวบรวมข้อมูลส่วนบุคคล ทั้งนี้ หลักการแจ้งให้ทราบทำให้ผู้ใช้บริการสามารถตัดสินใจบนพื้นฐานของการได้รับข้อมูลที่ครบถ้วนสมบูรณ์ว่าผู้ใช้บริการพอใจหรือไม่กับวิธีปฏิบัติในการเก็บรวบรวมข้อมูลของบริการออนไลน์นั้น นอกจากนี้กรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) ยังรับรองต่อไปด้วยว่าผู้ประกอบการบริการออนไลน์อาจใช้ข้อมูลที่ตนได้เก็บรวบรวมได้จากผู้ใช้บริการเท่าที่การใช้ดังกล่าวสอดคล้องกับข้อกำหนดที่ระบุไว้ในการแจ้งให้ทราบนั้น

หากมาตรา 26 ของร่าง พรบ. ถูกตีความโดยกำหนดให้ผู้ประกอบการบริการออนไลน์จะต้องขอรับความยินยอมแยกต่างหากก่อนใช้ข้อมูลส่วนบุคคล นอกเหนือจากการแจ้งให้ทราบล่วงหน้าเกี่ยวกับการเก็บรวบรวมและการใช้ข้อมูลตามวัตถุประสงค์ที่กำหนดไว้แล้ว ร่าง พรบ. นี้อาจสร้างภาระเป็นอย่างมากและไม่จำเป็นให้แก่ผู้ประกอบการ ผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล การตีความมาตรา 26 ดังกล่าวจึงขัดแย้งกับ “สมดุลที่สร้างขึ้นอย่างระมัดระวัง” (Carefully Struck Balance) ในกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) จึงควรมีการแก้ไขมาตรา 26 เพื่อให้เกิดความชัดเจนว่าเจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมสำหรับการใช้ข้อมูลของตนในภายหน้า โดยตกลงตามนโยบายคุ้มครองความเป็นส่วนตัวของบริการออนไลน์ หรือเลือกที่จะอยู่ภายใต้นโยบายดังกล่าว ที่จริงแล้วมีกลไกมากมายหลายอย่างที่ทำให้ผู้ใช้บริการสามารถจะควบคุมและให้ความยินยอมต่อการเก็บรวบรวมและใช้ข้อมูลของตนได้ และบางกลไกที่ผู้ใช้บริการเป็นผู้กำหนดทางเลือกของตนเอง (Opt-Out Mechanisms) ได้อย่างเต็มที่นั้น ทำให้เกิดคุ้มครองความเป็นส่วนตัวของผู้บริโภคในระดับที่สูงกว่า (โดยมีการรบกวนบ้างแก่ผู้ใช้บริการ

อินเตอร์เน็ต) กลไกที่ผู้ใช้บริการต้องเลือกที่จะอยู่ภายใต้นโยบายอย่างเดียว (Opt-In Mechanisms) ซึ่งให้การคุ้มครองความเป็นส่วนตัวที่ต่ำกว่า

เพื่อให้การตีความมาตรา 26 สอดคล้องกับกรอบการคุ้มครองความเป็นส่วนตัวของเอเปค (APEC Privacy Framework) บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาพิจารณาแก้ไขบทบัญญัติในข้อนี้ดังต่อไปนี้

> *ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ โอน หรือเปิดเผยข้อมูลส่วนบุคคลเพียงเพื่อปฏิบัติตามวัตถุประสงค์ของการเก็บรวมรวม และเพื่อวัตถุประสงค์ที่สอดคล้องกับวัตถุประสงค์ของการเก็บรวบรวมข้อมูล หรือวัตถุประสงค์ที่เกี่ยวข้องอื่น ตามที่ได้เปิดเผยต่อเจ้าของข้อมูลส่วนบุคคลตามมาตรา 22 ยกเว้นในกรณีต่อไปนี้*
>
> 1. *เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมแล้ว*
> 2. *จำเป็นต้องใช้ หรือเปิดเผยเพื่อให้บริการ หรือจัดหาผลิตภัณฑ์ซึ่งเจ้าของข้อมูลส่วนบุคคลร้องขอ*
> 3. *จำเป็นต้องใช้ หรือเปิดเผยเพื่อปฏิบัติหน้าที่ตามกฎหมาย*
> 4. *ข้อมูลส่วนบุคคลที่เก็บรวบรวมได้รับการเก็บรวบรวมตามข้อยกเว้นในมาตรา 23*

การโอนข้อมูลระหว่างประเทศ (มาตรา 27)

กรณีเป็นเรื่องเกี่ยวกับการไหลเวียนของข้อมูลข้ามพรมแดน มาตรา 27 จึงเป็นไปตามแนวทาง "ห้ามโอนเว้นแต่..." ของกฎหมายปัจจุบันว่าด้วยการคุ้มครองข้อมูลของสหภาพยุโรป (European Data Protection Directive) แนวทางดังกล่าวได้รับการวิพากษ์วิจารณ์อย่างมาก เนื่องจากขัดแย้งกับข้อเท็จจริงเรื่องการไหลเวียนของข้อมูลในประเทศต่างๆ ทั่วโลกที่เพิ่มมากขึ้นเรื่อยๆ ในช่วง 20 ปีที่ผ่านมา นับแต่มีการนำกฎหมายดังกล่าวมาใช้

นอกจากนี้ แนวทางเฉพาะที่กฎหมายของสหภาพยุโรปกำหนดไว้สำหรับการโอนข้อมูล เช่น แนวทางความเพียงพอ (Adequacy) แนวทางข้อสัญญา (Model Clauses) และแนวทางกฎเกณฑ์ที่มีผลผูกพันองค์กร (Binding Corporate Rules) ทำให้บริษัทต่างๆ ต้องผ่านกระบวนการที่ค่อนข้างซับซ้อนและใช้เวลามาก ซึ่งบริษัทส่วนมากไม่สามารถดำเนินการตามแนวทางเฉพาะดังกล่าวได้

ในโลกซึ่งมีการไหลเวียนของข้อมูลข้ามพรมแดน ต้องมีการกฎกติกาควบคุม (Rule) มากกว่าข้อยกเว้น (Exception) ข้อกำหนดทางกฎหมายจำเป็นต้องอยู่ในลักษณะที่บุคคลทุกคนซึ่งดูแลรักษาข้อมูลส่วนบุคคลสามารถปฏิบัติตามได้ภายในกรอบที่สมเหตุสมผล

ดังนั้น บีเอสเอจึงขอเสนอแนวทาง “ความรับผิดชอบ” (Accountability Model) ซึ่งแรกเริ่มนั้นโออีซีดี (OECD) กำหนดไว้ และต่อมาได้รับการรับรองและบูรณาการไว้ในระบบกฎหมายหลายระบบและหลักการคุ้มครองความเป็นส่วนตัวหลายหลักการ รวมถึงกรอบการควบคุมความเป็นส่วนตัวข้ามพรมแดนของเอเปค (Cross-Border Privacy Rules หรือ CBPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา (ซึ่งสหภาพยุโรปได้กำหนดว่าเพียงพอ) แนวทาง “ความรับผิดชอบ” (Accountability Model) จัดให้มีแนวทางที่นำไปสู่การกำกับดูแลข้อมูลข้ามพรมแดนซึ่งให้ความคุ้มครองแก่บุคคลอย่างมีประสิทธิภาพ และสนับสนุนการไหลเวียนของข้อมูลที่มีประสิทธิภาพเพิ่มขึ้น แนวทาง “ความรับผิดชอบ” (Accountability Model) กำหนดให้องค์กรต่าง ๆ ซึ่งเก็บรวบรวม และใช้ข้อมูล ต้องรับผิดชอบต่อการคุ้มครองข้อมูลและการใช้ข้อมูลอย่างมีความรับผิดชอบ ไม่ว่าจะมีการประมวลผลข้อมูล ณ ที่ใดหรือโดยผู้ใด นอกจากนี้ แนวทาง “ความรับผิดชอบ” (Accountability Model) ยังกำหนดว่าองค์กรที่ทำการโอนข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าได้มีการปฏิบัติตามภาระหน้าที่ต่างๆ ในทางกฎหมาย แนวทางปฏิบัติ หรือคำมั่นสัญญาที่ระบุไว้ในนโยบายคุ้มครองความเป็นส่วนตัว

ดังนั้น บีเอสเอจึงใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณาถึงประโยชน์และข้อด้อยของแนวทางทั้งหมดที่มี ก่อนจะตัดสินใจเลือกแนวทางที่เป็นที่สุด

หากเห็นควรต้องทำตามแนวทางของสหภาพยุโรป ก็ควรนำข้อยกเว้นเพิ่มเติมซึ่งได้มีการนำเสนอเป็นส่วนหนึ่งของการปฏิรูปกฎหมายอย่างต่อเนื่องในสหภาพยุโรปมาพิจารณาประกอบด้วย ข้อยกเว้นดังกล่าวมีวัตถุประสงค์ที่จะทำให้ระบบมีความยืดหยุ่นเพิ่มขึ้น เช่น ในขณะนี้มีการพิจารณารับรองข้อสัญญามาตรฐานที่มีอยู่ในสัญญาระหว่างผู้ประมวลผลหลายๆ ราย และอาจเป็นก้าวย่างที่ดีในการก้าวไปสู่การทำให้ระบบมีความยืดหยุ่นเพิ่มขึ้น อีกตัวอย่างคือความยืดหยุ่นที่เพิ่มขึ้นสำหรับการโอนข้อมูลระหว่างกลุ่มกิจการ หรือกลุ่มของวิสาหกิจซึ่งดำเนินการในกิจกรรมทางเศรษฐกิจร่วมกัน ซึ่งข้อเสนอใหม่นี้ได้พิจารณาอนุญาตให้ใช้กฎเกณฑ์ที่มีผลผูกพันองค์กร (Binding Corporate Rules) ที่ได้รับความเห็นชอบแล้ว สำหรับการโอนข้อมูลระหว่างประเทศของกลุ่มจากสหภาพยุโรปไปยังองค์กรต่าง ๆ ภายในกลุ่มบริษัทเดียวกัน หรือกลุ่มวิสาหกิจเดียวกัน ตราบที่กฎของกิจการนั้นมีหลักการที่สำคัญ และได้ระบุสิทธิที่บังคับใช้ได้ตามกฎหมายเพื่อให้มีการปกป้องคุ้มครองที่เหมาะสมสำหรับการโอนหรือประเภทของการโอนข้อมูลส่วนบุคคล

นอกจากนี้ ควรจะต้องมีระบบการรับรองร่วมกันเกี่ยวกับข้อกำหนดทางสัญญาที่เป็นมาตรฐาน และมาตรฐานของกิจการสากล (Global Corporate Standard) เพื่อหลีกเลี่ยงกรณีที่ข้อกำหนดในประเทศต่างๆ ทั่วโลกที่มีจำนวนมากและอาจขัดกัน เมื่อไม่นานมานี้คณะทำงานมาตรา 29 ของอียู

(EU's Article 29 Working Party) ได้ตีพิมพ์แนวทางปฏิบัติ (*WP 226*) ซึ่งจะกำหนดความแน่นอนให้มากขึ้นสำหรับบริษัทซึ่งโอนข้อมูลส่วนบุคคลออกนอกยุโรป

การเข้าถึงข้อมูล (มาตรา 28)

มาตรา 28 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้เกี่ยวกับตนเองได้ บีเอสเอเห็นด้วยว่าผู้ใช้บริการควรมีโอกาสศึกษาพิจารณาขอบเขตของข้อมูลที่เก็บรวบรวมไว้เกี่ยวกับตนเอง อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลต้องมีสิทธิหรือสามารถปฏิเสธคำร้องขอต่างๆ ได้ ในกรณีที่คำร้องขอดังกล่าวก่อให้เกิดภัยคุกคามต่อการรักษาความมั่นคงปลอดภัยของเครือข่าย ผู้ควบคุมข้อมูลส่วนบุคคลควรได้รับอนุญาตให้ไม่ต้องพิจารณาคำร้องขอที่เกี่ยวข้องกับข้อมูลที่เก็บรวบรวมไว้ หรือข้อมูลที่ใช้ ที่เกี่ยวข้องกับวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลและเครือข่าย หากไม่มีข้อยกเว้นดังกล่าว การปฏิบัติตามมาตรา 28 อาจก่อให้เกิดความเสี่ยงที่สูงขึ้นเกี่ยวกับการละเมิดข้อมูล ดังนั้นบีเอสเอจึงใคร่ขอเสนอให้มีการแก้ไขข้อความเป็นดังนี้

> *เจ้าของข้อมูลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่กรณีดังต่อไปนี้*
>
> 1. *เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมายอื่น หรือคำสั่งศาล*
> 2. *กระทบต่อความมั่นคงแห่งราชอาณาจักร*
> 3. *กระทบต่อเศรษฐกิจและการพาณิชย์ของประเทศ*
> 4. *มีผลต่อการสืบสวน สอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือการพิจารณาพิพากษาคดีของศาล*
> 5. *เพื่อคุ้มครองเจ้าของข้อมูล หรือสิทธิและเสรีภาพของบุคคลอื่น*
> 6. *<u>จะทำให้ความพยายามตามสมควรในการรักษาความมั่นคงปลอดภัยของข้อมูลและเครือข่ายลดลง</u>*

ความถูกต้องของข้อมูลส่วนบุคคล (มาตรา 30)

มาตรา 30 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการให้ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมไว้มีความถูกต้อง แม้ว่าผู้ให้บริการออนไลน์ได้รับประโยชน์ทางธุรกิจอย่างมากในการดำเนินการให้ข้อมูลที่ตนเก็บรวบรวมมีความถูกต้องก็ตาม แต่ความสามารถที่จะดำเนินการให้ข้อมูลมีความถูกต้องก็มีข้อจำกัด เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำให้

ข้อมูลส่วนบุคคลมีความทันสมัยได้ ก็ต่อเมื่อข้อมูลที่มีความทันสมัยได้ถูกจัดให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งบีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณาแก้ไขมาตรา 30 ดังนี้

> *ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ <u>เท่าที่สมควร</u> ให้ข้อมูลส่วนบุคคลนั้นถูกต้อง ทันสมัย สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด เว้นแต่จะมีกฎหมายกำหนดไว้เป็นอย่างอื่น*

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล - การแจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูล (มาตรา 31)

บีเอสเอสนับสนุนการสร้างระบบแจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลที่ใช้บังคับกับธุรกิจและองค์กรทั้งปวง บทบัญญัติที่กำหนดขึ้นอย่างเหมาะสมเกี่ยวกับการละเมิดข้อมูลจูงใจให้มีการนำวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เข้มแข็งมาใช้ และทำให้บุคคลธรรมดาสามารถที่จะดำเนินการเพื่อป้องกันตนเองในกรณีที่ข้อมูลของตนตกอยู่ในอันตราย ในการกำหนดบทบัญญัติเกี่ยวกับการแจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูลนั้น จะต้องพิจารณาว่าการละเมิดข้อมูลทุกครั้งมีอันตรายที่ไม่เท่ากัน ในหลายกรณีการละเมิดข้อมูลไม่ได้ก่อให้เกิดอันตรายจริงต่อบุคคลซึ่งข้อมูลของตนตกอยู่ในอันตราย

เพื่อไม่ให้ผู้บริโภคได้รับการแจ้งที่ไหลบ่าเข้ามาเพื่อให้ทราบเกี่ยวกับการละเมิดข้อมูลที่ไม่สำคัญ หน้าที่ในการแจ้งให้ทราบควรมีขึ้นเฉพาะในกรณีที่ก่อให้เกิดความเสี่ยงที่น่าเป็นไปได้อันอาจก่อให้เกิดความเสียหายต่อผู้ใช้บริการเท่านั้น ตัวอย่างเช่น หน้าที่ในการแจ้งให้ทราบไม่ควรเกิดขึ้นในกรณีที่ข้อมูลที่ถูกละเมิดนั้น บุคคลภายนอกที่ไม่ได้รับอนุญาตไม่สามารถใช้ได้ ไม่สามารถอ่านได้ หรือไม่สามารถถอดรหัสได้ผ่านวิธีปฏิบัติหรือวิธีการต่างๆ (เช่น การนำข้อความมาเข้ารหัส) ซึ่งเป็นที่ยอมรับอย่างกว้างขวางว่าเป็นวิธีปฏิบัติทางอุตสาหกรรมหรือมาตรฐานทางอุตสาหกรรมซึ่งมีประสิทธิภาพ และท้ายที่สุด เพื่อให้ผู้ใช้บริการได้รับการแจ้งให้ทราบที่มีความสำคัญในกรณีที่มีการละเมิด จึงจำเป็นเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องมีเวลาเพียงพอที่จะทำการประเมินความเสี่ยงได้อย่างละเอียดถี่ถ้วนเพื่อกำหนดขอบเขตของความเสี่ยงด้านความมั่นคงปลอดภัยและเพื่อป้องกันการเปิดเผยข้อมูลต่อเนื่องไปอีก ดังนั้นการกำหนดเวลาที่แน่นอนในการแจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูลอาจไม่ก่อให้เกิดผลดีนัก

จากที่กล่าวมาข้างต้น บีเอสเอใคร่ขอเสนอให้มีการพิจารณาแก้ไขดังต่อไปนี้ในมาตรา 31 (4)

แจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ซึ่งมีความเสี่ยงที่จะก่อให้เกิดความเสียหายอย่างสำคัญ แก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า และแจ้งให้ทราบถึงแผนการเยียวยาความเสียหายจากการละเมิดข้อมูลส่วนบุคคลนั้น

ในกรณีที่การละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงอันจะก่อให้เกิดความเสียหายอย่างสำคัญให้แก่บุคคลเกินกว่า 10,000 ราย ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งแก่คณะกรรมการทราบด้วย

ไม่ว่าในกรณีใดก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องแจ้งให้ทราบเกี่ยวกับการละเมิดหากข้อมูลที่ได้รับอันตรายได้รับการจัดเก็บไว้ในลักษณะที่ทำให้บุคคลภายนอกที่ไม่ได้รับอนุญาตไม่สามารถใช้ ไม่สามารถอ่าน หรือไม่สามารถถอดรหัสได้ผ่านวิธีปฏิบัติหรือวิธีการซึ่งเป็นที่ยอมรับกันในวงกว้างว่าเป็นวิธีปฏิบัติทางอุตสาหกรรม หรือมาตรฐานทางอุตสาหกรรมซึ่งมีประสิทธิภาพ

ความรับผิดทางแพ่ง (มาตรา 42)

เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการกระตุ้นอย่างเพียงพอในการดำเนินมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลตามสมควร จึงควรกำหนดความรับผิดทางแพ่งในกรณีมีการฝ่าฝืนพระราชบัญญัตินี้ อย่างไรก็ตาม ในการกำหนดกรอบความรับผิดทางแพ่ง ต้องตระหนักว่าแม้แต่มาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลที่แข็งแกร่งที่สุดก็สามารถถูกทำลายจากแฮกเกอร์ทางด้านอาชญากรรมที่มีความมุ่งมั่นได้ ดังนั้นจึงไม่เหมาะสมนักที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลมีความรับผิดในกรณีที่ขาดหลักฐานซึ่งแสดงว่าผู้ควบคุมข้อมูลส่วนบุคคลรายดังกล่าวฝ่าฝืนบทบัญญัติของพระราชบัญญัตินี้ซึ่งเป็นพระราชบัญญัติที่มีวัตถุประสงค์ที่จะกำหนดบรรทัดฐานทางกฎหมายในการเก็บรวบรวม ใช้ และคุ้มครองข้อมูลส่วนบุคคล บีเอสเอจึงใคร่ขอเสนอคณะกรรมการกฤษฎีกาโปรดพิจารณาแก้ไขมาตรา 42 ดังนี้

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ที่กำหนดไว้ในพระราชบัญญัตินี้เป็นเหตุใกล้ชิดของความเสียหายโดยตรงและความเสียหายที่เกิดขึ้นจริงกับเจ้าของข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการชดเชยเจ้าของข้อมูลส่วนบุคคลรายนั้นในจำนวนเท่ากับค่าความเสียหายโดยตรงและความเสียหายที่เกิดขึ้นจริง
ผู้ควบคุมข้อมูลส่วนบุคคลไม่ต้องรับผิดต่อความเสียหายซึ่งเกิดขึ้นจากเหตุดังต่อไปนี้

1. *เหตุสุดวิสัย*
2. *การกระทำตามคำสั่งของรัฐบาล หรือเจ้าพนักงานของรัฐ*

3. *การกระทำหรือละเว้นการกระทำของบุคคลที่เกี่ยวข้องหรือบุคคลอื่นนั้นเอง*
4. *การดำเนินการครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลซึ่งตนจัดทำขึ้นแล้ว*

ความรับผิดทางอาญา (มาตรา 43 - มาตรา 46)

ความรับผิดทางอาญาเป็นเรื่องเหมาะสมก็เมื่อเป็นกรณีที่เกี่ยวข้องกับการละเมิดกฎหมายอย่างร้ายแรงและจงใจ บีเอสเอมีความกังวลว่าบทบัญญัติเกี่ยวกับความรับผิดทางอาญาของร่างพระราชบัญญัติซึ่งร่างไว้ในเวลานี้อาจนำมาใช้บังคับในกรณีที่เกี่ยวกับการละเมิดกฎหมายเพียงเล็กน้อยหรือเป็นเหตุบังเอิญ เช่น มาตรา 44 ถือว่าการละเมิดหน้าที่ที่กำหนดไว้ในมาตรา 22 มาตรา 24 มาตรา 25 มาตรา 26 มาตรา 27 มาตรา 30 มาตรา 31 หรือ มาตรา 32 เป็นการกระทำความผิดทางอาญา กรณีอาจถือเป็นการละเมิดตามมาตรา 22 ได้ หากเว็บเพจซึ่งมีนโยบายเรื่องการคุ้มครองความเป็นส่วนตัวของผู้ควบคุมข้อมูลส่วนบุคคลใช้การไม่ได้ชั่วคราว ซึ่งทำให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถทำการแจ้งให้ทราบเกี่ยวกับนโยบายเรื่องการคุ้มครองความเป็นส่วนตัวได้อย่างเพียงพอแก่ผู้ใช้บริการเว็บไซต์นี้ การกำหนดความรับผิดทางอาญาในกรณีดังกล่าวเป็นเรื่องที่สร้างความกังวลเป็นอย่างยิ่ง ดังนั้น เพื่อให้การละเมิดซึ่งเป็นเพียงการละเมิดเชิงเทคนิคไม่ก่อให้เกิดความเสี่ยงต่อความรับผิดทางอาญา บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาแก้ไขมาตรา 44 เป็นดังนี้

> *ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตาม~~จงใจหรือเจตนาละเมิด~~มาตรา 22 วรรคหนึ่ง มาตรา 24 มาตรา 25 มาตรา 26 มาตรา 27 มาตรา 30 มาตรา 31 หรือมาตรา 32 <u>เพื่อผลประโยชน์ทางการเงินส่วนตัว หรือผลประโยชน์อื่น หรือมีความประสงค์จะสร้างความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล</u> ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ*
>
> *~~การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ~~*

บทบัญญัติที่มีข้อควรพิจารณาอย่างยิ่งคือ ร่างมาตรา 45 โดยมาตรานี้ถือว่าการกระทำซึ่งบทบัญญัติข้ออื่นในร่าง พรบ. อนุญาตไว้ให้กระทำได้ เป็นการกระทำความผิดทางอาญา เช่น ในขณะที่มาตรา 26 อนุญาตการใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลซึ่งได้รับ "ความยินยอม" จากเจ้าของข้อมูลส่วนบุคคล แต่มาตรา 45 (6) กลับกำหนดความรับผิดทางอาญาไว้ เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลจะได้รับ "ความยินยอมเป็นหนังสือ" และดังที่ได้หารือไว้ข้างต้นเกี่ยวกับมาตรา 26 ซึ่งกำหนดให้ผู้ควบคุม

ข้อมูลส่วนบุคคลต้องได้รับความยินยอมแต่ละคราวสำหรับการใช้ หรือการโอนข้อมูลส่วนบุคคลทุกคราวนั้นเป็นสิ่งที่ไม่สามารถทำได้ในความเป็นจริงในระบบของอินเตอร์เน็ตสมัยใหม่ ทั้งนี้ เทคโนโลยีแบบ Cloud-based และพาณิชย์อิเล็กทรอนิกส์ ในปัจจุบัน ต้องพึ่งพาความสามารถของผู้ให้บริการในการโอนข้อมูลที่ไม่มีการติดขัดเพื่อจัดหาผลิตภัณฑ์และบริการที่ผู้บริโภคต้องการให้แก่ผู้บริโภค เช่น หากบริษัทแห่งหนึ่งใช้ผู้ให้บริการด้านการทำบัญชีเงินเดือนผ่านทางออนไลน์ บริษัทต้องเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับพนักงานของตนแก่ผู้ให้บริการนั้น เพื่อที่พนักงานจะได้รับเงินตรงตามเวลา ซึ่งนี่เป็นเพียงหนึ่งตัวอย่างในหลายร้อยตัวอย่าง (หากไม่ใช่หลายพันตัวอย่าง) ของการใช้ข้อมูลส่วนบุคคลของแต่ละบุคคลซึ่งเกิดขึ้นเป็นรายวัน ดังนี้ บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาโปรดพิจารณาแก้ไขมาตรา 26 และมาตรา 45 เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ประโยชน์จากข้อมูลได้โดยชอบด้วยกฎหมาย (รวมทั้งการโอน และ/หรือ เปิดเผยข้อมูลดังกล่าว) เท่าที่ข้อมูลนั้นได้มีการเก็บรวบรวมไว้โดยเจ้าของข้อมูลส่วนบุคคลรับทราบแล้ว

บทสรุป

บีเอสเอขอแสดงความชื่นชมความพยายามส่งเสริมสิทธิในความเป็นส่วนตัว และเชื่อมั่นว่ากฎหมายที่ร่างขึ้นอย่างเหมาะสมจะนำไปสู่การบังคับใช้ที่มีประสิทธิภาพ บีเอสเอใคร่ขอให้คณะกรรมการกฤษฎีกาพิจารณาข้อคิดเห็นและข้อเสนอแนะดังกล่าวข้างต้นอย่างจริงจัง เพื่อนำมาซึ่งทางออกที่ดีที่สุดสำหรับทุกภาคส่วนที่เกี่ยวข้อง บีเอสเอยินดีเข้าพบเพื่อปรึกษาหารือกับคณะกรรมการกฤษฎีกาเพิ่มเติม หากมีคำถามหรือความเห็นประการใด กรุณาติดต่อ **คุณวารุณี รัชตพัฒนากุล ผู้แทนประจำประเทศไทยของบีเอสเอ ที่** varuneer@bsa.org **หรือ** +668-1840-0591

บีเอสเอขอขอบพระคุณที่คณะกรรมการกฤษฎีกาสละเวลาให้การพิจารณามา ณ ที่นี้

ขอแสดงความนับถือ

บูน โพ มอก (Boon Poh Mok)
ผู้บริหาร ฝ่ายนโยบาย ประจำภูมิภาคเอเชียแปซิฟิก (Director, Policy, APAC)
บีเอสเอ| พันธมิตรซอฟต์แวร์ (BSA | The Software Alliance)

สำเนาส่งถึง

๑. พณ. ท่าน ดร. วิษณุ เครืองาม รองนายกรัฐมนตรี

๒. นางสุรางคณา วายุภาพ ผู้อำนวยการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)