ข้อมูลประกอบการนำเสนอความเห็นและข้อเสนอแนะ แนวทางแก้ไขหรือปรับปรุง ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

5 เมษายน 2560

หน่วยงาน มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง

ชื่อผู้ให้ข้อมูล อาทิตย์ สุริยะวงศ์กุล

1 ระยะเวลาการมีผลบังคับใช้ของกฎหมาย (180 วันนับถัดจากวันประกาศราชกิจจานุเบกษา)

1.1 กรอบระยะเวลามีความเหมาะสมหรือไม่

- **บทบัญญัติที่เกี่ยวข้องกับคณะกรรมการคุ้มครองข้อมูลควรประกาศใช้ให้เร็วที่สุด ส่วนบทบัญญัติอื่นๆ สามารถทยอยให้มีผลบังคับใช้ตามความเหมาะสม ทั้งนี้ทั้งฉบับควรบังคับใช้ภายใน 180 วันนับถัดจากวันประกาศในราชกิจจานุเบกษา**

- เนื้อหาสาระหลักของร่างกฎหมายที่พิจารณาอยู่นี้ ส่วนใหญ่ยังเป็นไปตามที่ครม.เห็นชอบในหลักการตั้งแต่ต้นเดือนมกราคม 2558 และสำนักงานคณะกรรมกฤษฎีกาพิจาณาเสร็จตั้งแต่เดือนกรกฎาคม 2558 อีกทั้งผู้มีส่วนเกี่ยวข้องย่อมทราบว่าเป็นกฎหมายที่ถึงอย่างไรเสียก็ต้องมีอย่างหลีกเลี่ยงไม่ได้ มีการร่างมาหลายฉบับในหลายรัฐบาล อยู่ในวาระเศรษฐกิจดิจิทัลที่รัฐบาลปัจจุบันเป็นผู้ผลักดัน และเป็นส่วนหนึ่งของเงื่อนไขหรือข้อตกลงการค้าระหว่างประเทศ **ผู้เกี่ยวข้องมีเวลาเตรียมตัวเบื้องต้นมาไม่น้อยกว่า 2 ปีแล้ว**

- **การขอขยายเวลา (เพื่อการขอความยินยอมจากเจ้าของข้อมูลที่มีอยู่เดิม) อาจทำได้เป็นรายกรณี โดยอาจระบุหลักเกณฑ์และระยะผ่อนผันสูงสุดในบทเฉพาะกาล**

- ในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียนฉบับแรก ซึ่งดำเนินงานมาตั้งแต่ปี 2554 ได้กำหนดข้อริเริ่มที่ 2.4 คือ “การสร้างความเชื่อมั่น” โดยมี “การทำให้มั่นใจว่ามีการคุ้มครองข้อมูลส่วนบุคคล”[1] เป็นหนึ่งในรายละเอียดของแผนงานตามข้อริเริ่มดังกล่าว ตามยุทธศาสตร์ที่ 2 “การสร้างพลังและการมีส่วนร่วมของประชาชน” แผนแม่บทฯฉบับแรกดังกล่าวสิ้นสุดลงในปี 2558 ในรายงานประเมินผลภาพ

1 “Ensure personal data protection” – ASEAN ICT Masterplan 2015 หน้า 15 http://www.asean.org/storage/images/2012/Economic/TELMIN/ASEAN%20ICT%20Masterplan%202015.pdf

รวมทั้งภูมิภาคของการดำเนินงานตามแผนแม่บทระบุว่า “ปัจจัยหนึ่งที่ทำให้ประชากรจำนวนมากไม่ใช้บริการอิเล็กทรอนิกส์คือการขาดความเชื่อมั่น การดำเนินงานตามยุทธศาสตร์นี้ได้ช่วยทำให้ปัญหานี้ถูกจัดการด้วยการระบุถึงกฎหมายหรือกฎระเบียบที่จำเป็นต่อการสร้างความเชื่อมั่นที่ต้องมีเพื่อใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์”[2] ทั้งนี้แม้ประเทศไทยซึ่งเป็นชาติสมาชิกจะริเริ่มกระบวนการการออกหรือปรับปรุงกฎหมายที่จำเป็นแล้ว แต่ก็ยังไม่แล้วเสร็จ

- ในแผนแม่บทฯฉบับที่สอง การคุ้มครองข้อมูลถูกยกมาเป็นแผนงานที่ 8.1.1 ในยุทธศาสตร์ที่ 8 “ความมั่นคงและการประกันสารสนเทศ”[3] **ซึ่งมีกรอบเวลาเป้าหมายภายในไตรมาสที่ 2 ของปี 2560**
- สมควรให้กฎหมายมีผลบังคับใช้เร็วที่สุดหลังจากที่ประกาศแล้ว และไม่เกินภายในปี 2560 ก่อนที่ประเทศไทยจะเข้าสู่ช่วงกลางของแผนแม่บทฯฉบับที่สอง เนื่องจากยังมีกฎหมายลูกและกฎหมายที่เกี่ยวข้องที่จะต้องออกหรือแก้ไขให้สอดคล้องกับกฎหมายฉบับนี้อีก เพื่อไม่ให้ประเทศไทยพลาดเป้าหมายก่อนสิ้นสุดแผนแม่บทฯอีก และเพื่อให้ประชาชนได้มีความเชื่อมั่นโดยเร็วที่สุดกับการทำธุรกรรมอิเล็กทรอนิกส์

2 นิยาม ผู้ควบคุมข้อมูล

2.1 ความชัดเจนของนิยาม

- กรณีที่บุคคลหรือนิติบุคคลอาจไม่ได้มีอำนาจหน้าที่ตามกฎหมาย แต่ในทางปฏิบัติหรือตามข้อเท็จจริงเป็นผู้สามารถตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะถือว่าเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ตามนิยามของร่างปัจจุบันหรือไม่?

2.2 ควรเพิ่มเติมนิยามคำว่า “ผู้ประมวลผลข้อมูล” (Data Processor) หรือไม่

- **ควร** และควรเพิ่มเติมนิยามคำว่า “การประมวลผล” ให้ชัดเจนอีกคำหนึ่งด้วย เนื่องจากวลีว่า “การเก็บรวมรวม ใช้ หรือเปิดเผย” อาจไม่ครอบคลุมการประมวลผลทั้งหมด และเพื่อให้บทบัญญัติในส่วนอื่นๆ มีความกระชับ (ใช้คำว่า “การประมวลผล” ที่สั้นกว่า แทน “การเก็บรวมรวม ใช้ หรือเปิดเผย” ทั้งวลี)

2 ASEAN ICT Masterplan 2015 Completion Report หน้า 22 http://www.asean.org/storage/images/2015/December/telmin/ASEAN%20ICT%20Completion%20Report.pdf

3 “Information Security and Assurance” – ASEAN ICT Masterplan 2020 หน้า 26 และ 28 http://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

- ตัวอย่างนิยาม “ผู้ประมวลผล” (processor) จาก GDPR Article 4 (8): *““ผู้ประมวลผล” หมายความว่า บุคคลหรือนิติบุคคล, องค์การที่ใช้อำนาจสาธารณะ, สำนักงานหรือหน่วยงานอื่นใด ที่ประมวลผลข้อมูลส่วนบุคคล ในนามของผู้ควบคุม”*[4]

- ตัวอย่างนิยาม “ผู้ประมวลผลข้อมูล” (data processor) จาก UK DPA Section 1 (1): *““ผู้ประมวลผลข้อมูล” หมายความว่า บุคคลใด (นอกเหนือไปจากพนักงานของผู้ควบคุมข้อมูล) ที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล”*[5]

- ตัวอย่างนิยาม “การประมวลผล” (processing) จาก GDPR Article 4 (2): *““การประมวลผล” หมายความว่า การดำเนินการหรือชุดของการดำเนินการที่กระทำต่อข้อมูลส่วนบุคคล ไม่ว่าจะเป็นไปโดยอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม, การบันทึก, การจัดระเบียบ, การจัดโครงสร้าง, การเก็บรักษา, การปรับแปลงหรือดัดแปร, การกู้คืน, การพิจารณา, การใช้, การเปิดเผยโดยการส่ง เผยแพร่ หรือทำให้นำไปใช้ได้โดยวิธีอื่น, การเรียงหรือผสม, การจำกัด, การลบ, หรือการทำลาย”*[6] ซึ่งสอดคล้องกับนิยามใน Section 1 (1) ของ UK DPA

2.3 การแยกระหว่าง ผู้ควบคุมข้อมูล และ ผู้ประมวลผลข้อมูล

- กรณีที่รัฐกำหนดหน้าที่ให้เอกชนต้องประมวลผล (เก็บรวบรวม ใช้ เปิดเผย ฯลฯ) ข้อมูล เช่น เพื่อทำตามกฎในการกำกับกิจการ เพื่อบันทึกหลักฐานพยาน รัฐถือเป็นผู้ควบคุมข้อมูล และเอกชนถือเป็นผู้ประมวลข้อมูลที่ประมวลผลข้อมูลในนามของรัฐใช่หรือไม่?

- กรณีเช่นนี้ GDPR ได้ระบุไว้ในนิยามของผู้ควบคุมข้อมูลด้วย โดย Article 4 (7) บัญญัติว่าในกรณีที่วัตถุประสงค์หรือวิธีการในการประมวลผลนั้นถูกตัดสินใจโดยรัฐ รัฐสามารถบัญญัติกฎหมายเพิ่มเติมได้เพื่อระบุหลักเกณฑ์เฉพาะเจาะจงว่าใครจะถือเป็นผู้ควบคุมข้อมูลในกรณีดังกล่าว: *“‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; **where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;”***

4 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

5 http://www.legislation.gov.uk/ukpga/1998/29/section/1

6 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

3 หลักการให้ความยินยอม

3.1 การอนุญาตให้มีการให้ความยินยอมโดยปริยาย (deemed content)

4 หลักการเก็บรวบรวมข้อมูล

4.1 การเพิ่มข้อยกเว้นให้สามารถเก็บรวบรวมข้อมูลจากแหล่งอื่น รวมถึงการโอนข้อมูลที่ได้รับมาจากแหล่งอื่น และการให้ข้อมูลแก่บริษัทในกลุ่ม โดยไม่ต้องขอความยินยอม

- ต้องคำนึงถึงวัตถุประสงค์ที่เจ้าของข้อมูลให้ความยินยอมเป็นหลัก

5 หลักการใช้หรือการเปิดเผยข้อมูล

5.1 การเปิดเผยข้อมูลต่อบุคคลที่สาม (เพื่อผลประโยชน์/ความเสี่ยงต่อธุรกิจ)

- หากมีความเสี่ยงต่อธุรกิจอะไรที่จำเป็นจริงๆ ก็ควรจะระบุถึงความเสี่ยงดังกล่าวลงในกฎหมายเป็นการเฉพาะเลย ไม่ใช้คำว่า “ความเสี่ยงต่อ...” หรือ “ประโยชน์ต่อ...” เพราะเป็นคำที่กินความหมายกว้างมาก
- เช่นหากต้องการใช้เพื่อตรวจจับการฉ้อโกง หรือจำเป็นต้องเปิดเผยข้อมูลให้กับหน่วยงานกำกับกิจการเพื่อทำตามกฎหมาย ก็ให้ระบุเฉพาะกรณีดังกล่าวในกฎหมาย ซึ่งแนวทางนี้เป็นแนวทางที่อุตสาหกรรมในประเทศอื่นก็เสนอเช่นกัน เช่น ความเห็นที่สมาคมผู้รับประกันแห่งสหราชอาณาจักรมีต่อการตีความ “Legitimate Interests” ใน Article 7 (f) ของ Directive 95/46/EC (Data Protection Directive)[7]
- กรณีการประมวลผลข้อมูลเพื่อประเมินคุณลักษณะของบุคคล GDPR เปิดช่องให้ทำได้ โดยเรียกกระบวนการดังกล่าวว่า **“profiling”** โดยนิยามว่า *“‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;”*[8] และมีบทบัญญัติเกี่ยวกับเรื่องดังกล่าวเป็นการเฉพาะ

7 Association of British Insurers (June 2014) http://ec.europa.eu/justice/data-protection/article-29/press-material/public-consultation/notion-legitimate-interests/files/abi_response_to_article_29_working_party_opinion_06-2014_on_legitimate_interests.pdf

8 GDPR Article 4 (4) http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

5.2 ความเหมาะสมของข้อยกเว้น

5.3 การนำข้อมูลบางส่วนหรือที่ไม่สามารถบ่งบอกตัวตนมาใช้งานได้ โดยไม่ต้องขอความยินยอม

- กรณีนำข้อมูลที่ไม่สามารถระบุตัวตนได้ไปวิเคราะห์ต่อ อาจพิจารณาให้ทำได้ด้วยความระมัดระวังโดยไม่ต้องขอความยิมยอมอีกครั้ง แต่ก็ต่อเมื่อสามารถแสดงให้เห็นได้ว่าข้อมูลที่ใช้ระบุบุคคลได้ไม่ว่าจะโดยตรงหรือโดยอ้อมได้ถูกลบออกไปหมดแล้วโดยแท้จริงและไม่สามารถเชื่อมโยงกลับอีกครั้งได้ ตามมาตรฐานทางเทคนิคและมาตรฐานการจัดการองค์กรที่เป็นที่ยอมรับของอุตสาหกรรซึ่งได้รับการรับรองจากคณะกรรมการคุ้มครองข้อมูล (กระบวนการนี้มักเรียกว่า “deidentification” หรือ “anonymization” แต่ใน GDPR จะเรียกว่า “pseudonymisation”[9] เนื่องจากมองว่าไม่มีกระบวนการใดที่ทำให้เป็นนิรนามได้สมบูรณ์)

- มาตรการการคุ้มครองข้อมูลที่เคยเชื่อกันว่าใช้ได้ในอดีต อาจใช้ไม่ได้อีกต่อไปในปัจจุบัน เนื่องจากมันถูกออกแบบมาเพื่อใช้ในบริบทข้อจำกัดทางเทคโนโลยีแบบหนึ่ง ซึ่งไม่เป็นจริงอีกต่อไปแล้ว การออกแบบนโยบายและมาตรการต่างๆ รวมถึงข้อบังคับและข้อยกเว้นในกฎหมายคุ้มครองข้อมูล ควรตั้งอยู่บนฐานของเทคโนโลยีในปัจจุบันและความเป็นไปได้ทางเทคโนโลยีในอนาคต ที่อาจกระทบกับเจ้าของข้อมูล[10]

- มาตรการทางเทคโนโลยีที่ออกแบบผิดพลาดเป็นอันตรายอย่างยิ่ง เนื่องจากทำให้ผู้ใช้เชื่ออย่างผิดๆ ว่าเป็นมาตรการที่ใช้งานได้จริง ตัวอย่างเช่นมาตรฐานการเข้ารหัสที่ออกแบบมาอย่างไม่ระมัดระวังและนำไปใช้กับฐานข้อมูลการจ่ายยาผู้ป่วยในเกาหลีใต้ ทำให้ข้อมูลทั้ง 100% ถูกระบุตัวตนกลับได้[11]

- การเข้ารหัสลับข้อมูล (encryption) การลดข้อมูลให้เหลือน้อยที่สุดเท่าที่จะเพียงพอกับวัตถุประสงค์ (data minimization) การแบ่งส่วนข้อมูลเป็นชิ้นย่อย (data segmentation) การนำข้อมูลระบุตัวตนออกจากข้อมูล (pseudonymization) และการพรางข้อมูลส่วนบุคคล (data masking/data obfuscation)[12] เป็นมาตรการทางเทคโนโลยีที่สามารถใช้ปรับใช้ร่วมกันเพื่อให้สามารถใช้งานข้อมูลเพื่อประโยชน์สาธารณะโดยที่ยังคุ้มครองเจ้าของข้อมูลอยู่ – ประเด็นปัญหาคือ จะทราบได้อย่างไรมาตรการทางเทคโนโลยีแบบใดที่จะเพียงพอต่อการคุ้มครองข้อมูล เรื่องนี้น่าจะเป็นงานที่คณะกรรมการคุ้มครองข้อมูลสามารถพิจารณาได้ต่อไป

---

9 GDPR Article 4 (5) http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

10 การคุ้มครองข้อมูลส่วนบุคคลในระบบสุขภาพ https://prachatai.com/journal/2015/05/59373

11 De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data http://techscience.org/a/2015092901/ และ South Korea: Medical data delivers yet another identity crisis https://nakedsecurity.sophos.com/2015/10/05/south-korea-yet-another-identity-crisis/

12 Data masking/Data obfuscation เป็นกระบวนการทำให้การหาความเชื่อมโยงเพื่อระบุตัวตนกลับทำได้ยากขึ้น กระบวนการนี้จะเพิ่มข้อมูลสุ่มเข้าไปในชุดข้อมูล หรือแทนที่ข้อมูลดั้งเดิมบางส่วนด้วยข้อมูลที่ใช้งานได้เหมือนกันสำหรับวัตถุประสงค์หนึ่งแต่ไม่ระบุถึงบุคคล อย่างไรก็ตามเพื่อที่จะยังสามารถใช้ประโยชน์จากชุดข้อมูลดังกล่าวในเชิงสถิติได้ ข้อมูลสุ่มที่เพิ่มเข้าไปจะถูกสุ่มขึ้นมาให้มีการกระจายเชิงสถิติใกล้เคียงกับชุดข้อมูลจริงในภาพรวม ชุดข้อมูลผลลัพธ์จะเป็นชุดข้อมูลที่มีทั้งข้อมูลสุ่มและข้อมูลจริง ทำให้หาความเชื่อมโยงกลับไปยังบุคคลได้ยากขึ้น แต่ยังมีความถูกต้องในเชิงสถิติอยู่ – Implement Data Masking to Protect Sensitive Data http://www.ibmbigdatahub.com/blog/implement-data-masking-protect-sensitive-data-part-1 และ http://www.ibmbigdatahub.com/blog/implement-data-masking-protect-sensitive-data-part-2

5.4 การเพิ่มเติมข้อยกเว้น เช่น ประเภทประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

- การอนุญาตให้ประมวลผลข้อมูลได้เพื่อประโยชน์โดยชอบธรรมของผู้ควบคุมข้อมูลหรือของบุคคลที่สาม เป็นสิ่งที่ทั้ง Data Protection Directive และ GDPR อนุญาตให้ทำได้-ก็ต่อเมื่อประโยชน์ดังกล่าวไม่ขัดกับประโยชน์ที่จะมีต่อสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล การอนุญาตในกรณีนี้จึงเป็นการอนุญาตที่จะทำได้ก็ต่อเมื่อมีการทำ “balancing test” ชั่งน้ำหนักประโยชน์ต่างๆ เป็นรายกรณี[13]

- นอกจากนี้ในกรณีของ GDPR ยังเน้นถึงกรณีที่เจ้าของข้อมูลเป็นเด็ก และยังมีเงื่อนไขกำกับด้วยว่า การอ้างประโยชน์โดยชอบธรรมของผู้ควบคุมข้อมูลดังกล่าว จะต้องไม่ใช่การประมวลผลข้อมูลโดยหน่วยงานที่ใช้อำนาจรัฐ (public authority) และเนื่องจากการประมวลผลดังกล่าวไม่ได้ตั้งอยู่บนฐานของวัตถุประสงค์ที่เจ้าของข้อมูลให้ความยินยอม การประมวลผลดังกล่าวจึงต้องทำตาม Article 6.4 อีกด้วย โดยอนุมาตราดังกล่าวระบุถึงข้อพิจารณา 6 ข้อที่ใช้กำกับการประมวลผลข้อมูลเพื่อให้วัตถุประสงใหม่ดังกล่าวยังสอดคล้อง (compatible) ไม่ขัดกับวัตถุประสงค์ที่เจ้าของข้อมูลยินยอมในตอนแรก ข้อพิจารณาดังกล่าวได้แก่

    - (a) ความเชื่อมโยงระหว่างวัตถุประสงค์ในตอนที่เก็บรวบรวมข้อมูลส่วนบุคคลมาและวัตถุประสงค์ที่ตั้งใจจะประมวลต่อไป

    - (b) บริบทในตอนที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวมมา โดยเฉพาะความสัมพันธ์ระหว่างเจ้าของข้อมูลและผู้ควบคุม [เช่น เจ้าของข้อมูลอยู่ในฐานะที่จะปฏิเสธไม่ให้เก็บข้อมูลได้มากน้อยเพียงใด]

    - (c) ธรรมชาติของข้อมูลส่วนบุคคลดังกล่าว โดยเฉพาะว่ามันเป็นข้อมูลส่วนบุคคลประเภทพิเศษตาม Article 9 [เช่น ข้อมูลอ่อนไหว] หรือข้อมูลเกี่ยวกับอาชญากรรมตาม Article 10 หรือไม่

    - (d) ผลกระทบที่เป็นไปได้ว่าจะเกิดขึ้นกับเจ้าของข้อมูลหากมีการประมวลผลข้อมูลต่อไปอย่างที่ตั้งใจ

    - *(e) การดำรงอยู่ของมาตรการการป้องกันที่เหมาะสม ซึ่งอาจรวมถึงการเข้ารหัสลับ (encryption) หรือการทำให้ข้อมูลเชื่อมโยงไปถึงบุคคลไม่ได้อีกต่อไป (pseudonymisation)*

- Data Protection Directive Article 7 (f): *“Member States shall provide that personal data may be processed only if: […] (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed,* ***except where such interests are overridden by the interests for***

13 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (Adopted on 9 April 2014) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

fundamental rights and freedoms of the data subject which require protection under Article 1 (1). *"*

- GDPR Article 6.1 (f): *"Processing shall be lawful only if and to the extent that at least one of the following applies: [...] (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,* ***except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.***

  Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks*"*

- GDPR Article 6.4 "***Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent*** *or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1),* ***the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:***

  (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

  (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

  (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

  (d) the possible consequences of the intended further processing for data subjects;

  (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

- โปรดสังเกตด้วยว่าทั้งใน Data Protection Directive และ GDPR จะไม่เรียกหลักเกณฑ์เหล่านี้ว่าเป็น “ข้อยกเว้น” โดย Data Protection Directive จะเรียกว่า “หลักเกณฑ์ที่ทำให้การประมวลผลข้อมูลมีความชอบธรรม” (Criteria for Making Data Processing Legitimate – Section II) ส่วนใน GDPR จะเรียกว่า “ความชอบด้วยกฎหมายของการประมวลผล” (Lawfulness of processing – Article 6) ทั้งนี้หมายความว่า ข้อมูลในประเภทนี้แม้จะอนุญาตให้ประมวลผลได้ แต่ก็ยังต้องทำตามหลักการอื่นๆ ในกฎหมายด้วย ไม่ใช่ถือว่าเป็นข้อยกเว้นและไม่ต้องทำตามหลักการอื่นๆ ที่เหลือในกฎหมายเลย

6 สิทธิของเจ้าของข้อมูล

6.1 การทำลายข้อมูล และการถอนความยินยอม (บางกรณีจำเป็นต้องเก็บเพื่อประโยชน์ในการดำเนินคดีในอนาคต แต่ไม่สามารถนำข้อมูลไปใช้ต่อได้)

6.2 การเพิ่มเติมข้อยกเว้นในมาตราที่เกี่ยวข้อง (ม. 30, ม. 21)

- การเขียนกฎหมายว่าให้เพิ่มเติมข้อยกเว้นได้โดยออกเป็นกฎหมายลูกเพิ่มเติม ควรเขียนกำกับหลักเกณฑ์หรือข้อพิจารณาให้ชัดเจนว่ากฎหมายลูกจะต้องอยู่ในกรอบใดบ้าง – แม้โดยหลักการทั่วไป กฎหมายลูกจะไม่สามารถขัดกับกฎหมายหลักได้อยู่แล้ว แต่เพื่อความชัดเจนเนื่องจากกรณีนี้เกี่ยวกับสิทธิเสรีภาพพื้นฐานที่สำคัญของประชาชน ที่กฎหมายลูกดังกล่าวอาจทำให้เสียสิทธิเสรีภาพดังกล่าวไป จึงเห็นสมควรเขียนกำหนดกรอบย้ำอีกครั้ง

7 บทเฉพาะกาล

7.1 การใช้งานข้อมูลที่เก็บรวบรวมไว้ก่อนที่กฎหมายฉบับนี้จะมีผลใช้บังคับให้สามารถใช้งานได้โดยไม่ต้องขอความยินยอม

- ถ้าวัตถุประสงค์ในการใช้ข้อมูลหรือผู้ควบคุมข้อมูลมีการเปลี่ยนแปลงไปจากเมื่อครั้งแรกที่เก็บรวบรวมข้อมูลมา ต้องขอความยินยอมใหม่ ไม่เช่นนั้นจะใช้ผู้ควบคุมข้อมูลใหม่จะต้องทำลายข้อมูล หรือผู้ควบคุมข้อมูลเดิมจะใช้เพื่อวัตถุประสงค์ใหม่ไม่ได้ – ทั้งนี้ข้อมูลส่วนบุคคลที่เก็บอยู่แล้วดังกล่าวจะต้องไม่ใช่ข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal data) และวัตถุประสงค์ในการใช้ข้อมูลต้องไม่ขัดกับกฎหมายใหม่
- ถ้าวัตถุประสงค์ในการใช้ข้อมูลหรือผู้ควบคุมข้อมูลไม่มีการเปลี่ยนแปลงไปจากเมื่อครั้งแรกที่เก็บรวบรวมข้อมูลมา ต้องขอความยินยอมใหม่เช่นกัน แต่ผู้ควบคุมข้อมูลอาจขอผ่อนผันกับคณะกรรมการคุ้มครองข้อมูลได้ โดยในการขอผ่อนผันต้องแสดงแผนการดำเนินงานและระยะเวลาที่คาดว่าจะแล้วเสร็จ – ทั้งนี้ข้อมูลส่วน

บุคคลที่เก็บอยู่แล้วดังกล่าวจะต้องไม่ใช่ข้อมูลส่วนบุคคลที่อ่อนไหว วัตถุประสงค์ในการใช้ข้อมูลต้องไม่ขัดกับกฎหมายใหม่ และระยะเวลาที่ขอผ่อนผันรวมจะต้องไม่เกินหลักเกณฑ์ระยะเวลาผ่อนผันกลางที่กำหนดในบทเฉพาะกาล เช่น ภายใน 2 ปี – โดยในระหว่างนั้น ผู้ควบคุมข้อมูลอาจประชาสัมพันธ์ให้เจ้าของข้อมูลติดต่อเข้ามารับทราบวัตถุประสงค์และเงื่อนไขการใช้ข้อมูลส่วนบุคคลและตัดสินใจให้ความยินยอมใหม่ (opt-in) ถ้าหมดช่วงเวลาผ่อนผันและยังไม่ได้รับความยินยอมจากเจ้าของข้อมูล ต้องทำลายข้อมูลทิ้ง

8 อื่นๆ

8.1 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ประเด็นระยะเวลาในการแจ้งให้ทราบเกี่ยวกับการละเมิดข้อมูล

8.2 การพิจารณากรอบความเป็นส่วนตัวของ APEC (APEC Privacy Framework) และเรื่อง APEC Cross Border Privacy Rule (CBPR)

- การนำ APEC Privacy Framework มาใช้ควรพิจารณาปีที่กรอบดังกล่าวออกมาด้วย คือปี 2548 (เริ่มร่างปี 2546 adopted ปี 2547 finalized ปี 2548) ซึ่งในตอนนั้น Facebook กับ Gmail เพิ่งเปิดได้หนึ่งปีและยังไม่เปิดให้บุคคลทั่วไปลงทะเบียน ในฝั่งผู้ใช้ สมาร์ตโฟนยังไม่มีทั้ง iPhone (ออกปี 2550) และ Android (ออกปี 2551) ในฝั่งเซิร์ฟเวอร์หรือระบบคลาวด์ Amazon Web Services ยังไม่มี (ออกปี 2549) สภาพเศรษฐกิจ สังคม และเทคโนโลยีเมื่อ 12 ปีที่แล้วที่ APEC Privacy Framework ออกมานั้น แตกต่างอย่างมากจากสภาพในปัจจุบัน – ในขณะที่ General Data Protection Regulation ของสหภาพยุโรปซึ่งออกมาในปี 2559 ได้พยายามแก้ไขประเด็นปัญหาใหม่ๆ ที่เพิ่งเกิดขึ้นในทศวรรษที่ผ่านมาและเป็นปัญหาที่ Data Protection Directive ของสหภาพยุโรปเองแต่เดิมยังไม่ได้เขียนระบุไว้อย่างชัดเจน
- ใน CBPR มีการกำหนด Accountability Agent ที่จะทำหน้าที่ตรวจสอบบริษัทที่ได้รับการรับรอง ภาระงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจต้องคำนึงถึงส่วนที่จะต้องรับเรื่องร้องเรียนจาก Accountability Agent ด้วย

8.3 ข้อมูลที่พระราชบัญญัติไม่ใช้บังคับ (ร่างมาตรา 4)

- ข้อยกเว้น *"(4) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์* ***รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา****"* เป็นข้อยกเว้นที่กว้างเกินไปมาก ทำให้ประชาชนไม่ได้รับความคุ้มครองใดๆ จากกฎหมายนี้เลย และจะไม่สามารถ

ร้องเรียนต่อคณะกรรมการคุ้มครองส่วนบุคคลได้หากพบการละเมิดข้อมูลส่วนบุคคลในระหว่างกระบวนการยุติธรรมทางอาญา – การยกเว้นควรกำหนดอย่างเฉพาะเจาะจง เพื่อให้เจ้าหน้าที่สามารถทำงานได้และการคุ้มครองตามสิทธิโดยทั่วไปก็ยังคงใช้บังคับได้อยู่ – ตัวอย่างเช่น Section 29 ของ Data Protection Act 1998 ของสหราชอาณาจักร ที่ว่าด้วยข้อยกเว้นของกฎหมายในกิจการเกี่ยวกับ "อาชญากรรมและภาษี"[14] ได้ระบุว่าให้ยกเว้นไม่นำหลักการการคุ้มครองข้อมูลข้อที่ 1 (ดังที่ระบุไว้ใน Schedule 1 จำนวน 8 ข้อ[15]) ซึ่งเกี่ยวกับเงื่อนไขและความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลที่อ่อนไหวมาใช้บังคับกับเรื่องดังกล่าว โดยที่หลักการการคุ้มครองข้อมูลที่เหลืออีก 7 ข้อ (เช่น หลักการความถูกต้องของข้อมูล หลักการความเพียงพอและไม่เกินความจำเป็นของข้อมูล) ยังใช้บังคับอยู่

- การยกเว้นในมาตรา 4 (2) (3) (5) และ (6) ก็เช่นกัน หากเห็นว่ามีความจำเป็นควรยกเว้นเฉพาะบางมาตราอย่างเฉพาะเจาะจง ไม่ใช่การยกเว้นไม่ใช้บังคับทั้งฉบับ เพื่อให้กฎหมายฉบับนี้คงความเป็นกฎหมายกลางที่บังคับใช้กับทุกกิจการอย่างเท่าเทียม

- สิทธิในความเป็นอยู่ส่วนตัวและเสรีภาพในการติดต่อสื่อสารกัน เป็นสิทธิและเสรีภาพตามรัฐธรรมนูญ[16] การกำหนดข้อยกเว้นเพิ่มเติมไม่ให้นำพระราชบัญญัติฉบับนี้มาใช้บังคับ ควรทำโดยกฎหมายระดับพระราชบัญญัติที่มีศักดิ์เท่ากันหรือไม่ – เสนอแก้ไขวรรคสองของมาตรา 4 เป็น *"การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใดหรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ~~หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา~~ จะทำได้ก็ต่อเมื่อพิจารณาแล้วว่ามีความจำเป็นเพื่อการคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อคุ้มครองสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้ให้ตราเป็นพระราชบัญญัติ"*

8.4 ข้อยกเว้นในนิยามข้อมูลส่วนบุคคล (ร่างมาตรา 3)

- ข้อยกเว้นเรื่องชื่อหรือสถานที่ทำงานฯ ตามนิยามของร่างปัจจุบัน – *""ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม* ***แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ*** *และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ"* – ในร่างไม่ชัดเจนว่าต้องการยกเว้นเพื่อวัตถุประสงค์ใดและในบันทึกประกอบร่างของสคก.ก็ไม่ได้มีอธิบายเอาไว้ – เสนอว่าไม่ควรมีข้อยกเว้นลักษณะนี้ในตัวนิยาม แต่หากเห็นว่าจำเป็นในกรณีใดหรือกิจการใด ก็ให้บัญญัติการยกเว้นเป็นการเฉพาะกรณีนั้นหรือกิจการนั้น – เมื่อสำรวจนิยามข้อมูลส่วนบุคคลในกฎหมายหรือกรอบ

14 http://www.legislation.gov.uk/ukpga/1998/29/section/29

15 http://www.legislation.gov.uk/ukpga/1998/29/schedule/1

16 ร่างรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ..... (ฉบับผ่านประชามติ 7 ส.ค. 2559) มาตรา 32 และมาตรา 36

ดำเนินงานอย่าง OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, UK Data Protection Act 1998, EU General Data Protection Regulation, และ APEC Privacy Framework ก็ไม่พบบัญญัติการยกเว้นลักษณะดังกล่าวไว้ในนิยาม

8.5 ความเป็นอิสระและทรัพยากรของคณะกรรมการคุ้มครองข้อมูล

- เพื่อให้คณะกรรมการสามารถทำงานคุ้มครองได้จริง จำเป็นต้องออกแบบโครงสร้างให้รับประกันความอิสระในการทำงานของคณะกรรมการ – คณะกรรมการมีอำนาจเพียงพอที่จะทำงานตามหน้าที่ที่ได้รับมอบหมาย – รวมถึงคณะกรรมการจำเป็นต้องมีบุคคลากรและทรัพยากรเป็นของตัวเองในปริมาณที่เหมาะสมกับภาระงานด้วย[17]

- ข้อสังเกตโครงสร้างคณะกรรมการในร่างปัจจุบัน

    - โครงสร้าง: คณะกรรมการอยู่ภายใต้โครงสร้างกระทรวง (มาตรา 6)

    - ที่มากรรมการ: ฝ่ายการเมือง (คณะรัฐมนตรี) มีอำนาจโดยตรงและโดยอ้อมในการเลือกกรรมการ (มาตรา 7) – ประธาน แต่งตั้งและให้ออกโดยคณะรัฐมนตรี, กรรมการโดยตำแหน่ง 5 จาก 7 คนเป็นปลัดกระทรวงหรือผู้บริหารระดับกรม, กรรมการผู้ทรงคุณวุฒิ 5 คน แต่งตั้งโดยคณะรัฐมนตรี

    - ภาระงาน-การขัดประโยชน์: กรรมการไม่ได้ทำงานเต็มเวลา และอาจทำงานให้องค์กรรัฐ/เอกชนอื่นด้วย

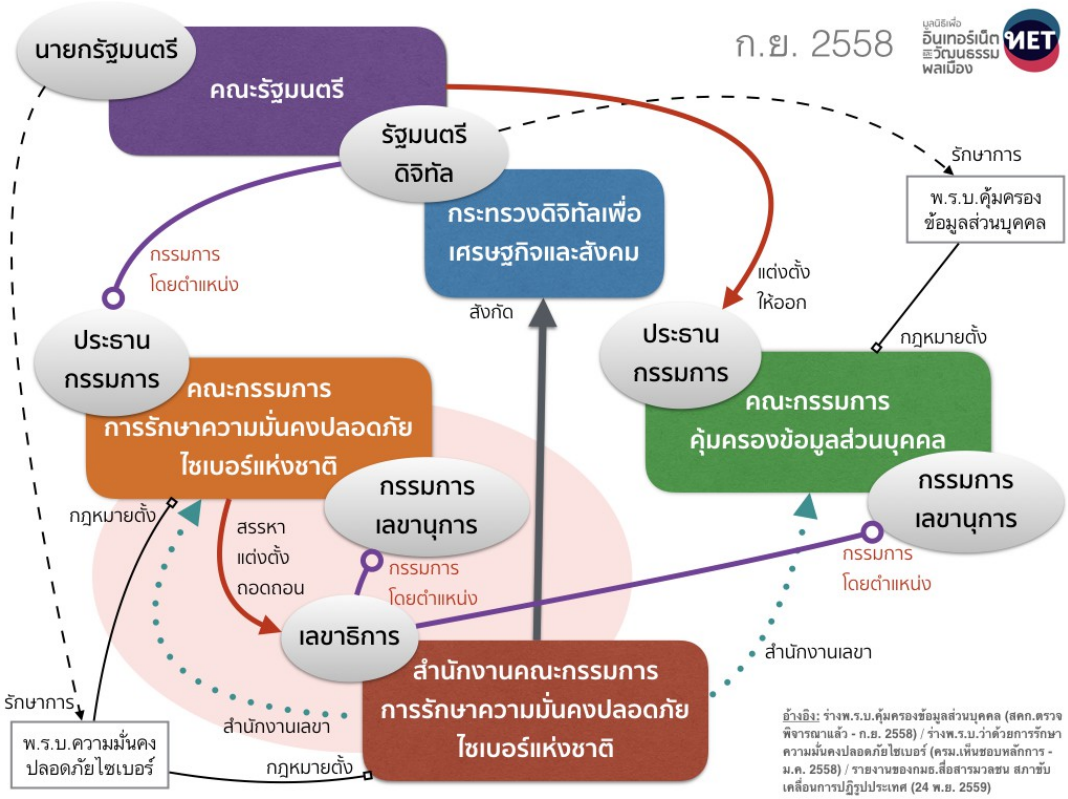
    - ทรัพยากร-ดุลอำนาจ: ไม่มีสำนักงานเฉพาะเป็นของตัวเอง ต้องพึ่งพาทรัพยากรและบุคลากรของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการปฏิบัติงาน (มาตรา 7, 16)

        - ภาระหน้าที่ของ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ และ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล บางส่วนอาจส่งเสริมกัน บางส่วนในบางเวลาอาจขัดกัน

        - เจ้าหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ รายงานต่อเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (ซึ่งแต่งตั้งและถอดถอนโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์) คำถามคือในกรณีที่สองคณะกรรมการนี้มีความเห็นขัดกัน เจ้าหน้าที่ของสำนักงานจะตกอยู่ในความกดดันหรือไม่หรือจะตัดสินใจทำงานให้กับใคร

17 ออกแบบหน่วยงานคุ้มครองข้อมูลที่มีประสิทธิภาพ: บทเรียนจากสหภาพยุโรป https://bact.cc/2017/eu-data-protection-authority-best-practices/

โครงสร้างเชิงอำนาจของหน่วยงานต่างๆ ที่สัมพันธ์กับการคุ้มครองข้อมูลส่วนบุคคล ตามร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (ก.ย. 2558) และร่างพ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (ม.ค. 2558)



โครงสร้างเชิงอำนาจของหน่วยงานต่างๆ ที่สัมพันธ์กับการคุ้มครองข้อมูลส่วนบุคคล ตามร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (ก.ย. 2558) ล่าสุดและข้อเสนอของสภาขับเคลื่อนการปฏิรูปประเทศ (พ.ย. 2559)