

รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐ
ภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล*
SUITABLE PRIVATE DATA SHARING FOR GOVERNMENT MANAGEMENT
UNDER THE PERSONAL DATA PROTECTION ACT

พงษ์มนัส ดีอด

Pongmanut Deeod

พระครูวินัยธรวรชาติ ปยุตโต

Phrakhru Winaithon Worachad Payutto

ปาริฉัตร ไชยเดช

Parichat Chaiyadat

พระมหาชัยชนะ บุญนาดี

Phramaha Chaichana Boonnadee

มหาวิทยาลัยมหามกุฏราชวิทยาลัย วิทยาเขตอีสาน

Mahamakut Buddhist University Isan Campus, Thailand

E-mail: pongmanut.dee@gmail.com

บทคัดย่อ

บทความฉบับนี้ศึกษาถึงรูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เนื่องจากข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนขั้นพื้นฐาน ที่รัฐพึงดูแล เป็นหลักประกันแก่ประชาชน อย่างไรก็ตามเมื่อรัฐต้องการเข้าสู่รัฐบาลดิจิทัล ซึ่งข้อมูลทุกอย่างของประชาชนจะต้องมีการเชื่อมโยงข้อมูลหรือจัดการร่วมกันระหว่างหน่วยงานมากยิ่งขึ้น เพื่อการวิเคราะห์ข้อมูลและวางแผนก่อให้เกิดนโยบายที่เหมาะสมกับประชาชน แต่เมื่อพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีการแบ่งปันข้อมูลในประเทศไทยนั้น จะเห็นได้ว่ายังไม่มีรูปแบบที่ชัดเจนในการวางมาตรฐานการแบ่งปันข้อมูลในภาครัฐ จึงจำเป็นต้องพิจารณาร่วมกับกฎหมายต่างประเทศจะพบได้ว่า ในประเทศญี่ปุ่นนั้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อนที่จะมีการแบ่งข้อมูลส่วนบุคคล หรือก่อนที่มีการใช้ข้อมูลส่วนบุคคลได้จะต้องยินยอม เว้นแต่มีข้อยกเว้นหากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถานการณ์นั้นที่เกิดขึ้น ประเทศสิงคโปร์ได้แบ่งวิธีการโอนข้อมูลส่วนบุคคลออกเป็น 2 ลักษณะ คือ 1)

* Received May 13, 2022; Revised June 27, 2022; Accepted July 18, 2022

มาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ 2) มาตรการแบ่งปันข้อมูลส่วนบุคคลให้กับต่างประเทศ และสำหรับกลุ่มสหภาพยุโรปได้แบ่งรูปแบบการแบ่งปันข้อมูลส่วนบุคคลออกเป็น 2 กรณีกล่าวคือ 1) การแบ่งปันข้อมูลส่วนบุคคลกับบุคคลหรือหน่วยงานที่สามเพื่อใช้ในวัตถุประสงค์ร่วมกันภายในสหภาพยุโรป 2) การแบ่งปันที่เกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนบุคคลสหภาพยุโรปหรือองค์การระหว่างประเทศ ซึ่งรูปแบบการคุ้มครองข้อมูลส่วนบุคคล ดังนี้ ประเทศไทยนำรูปแบบการคุ้มครองสำหรับแบ่งปันข้อมูลส่วนบุคคลมาพิจารณาประกอบไปด้วย

คำสำคัญ: กฎหมายคุ้มครองข้อมูลส่วนบุคคล, การแบ่งปันข้อมูล, การบริหารงานภาครัฐ

Abstract

The purpose of this article is to investigate the suitable way to share personal data for government management under private data preservation because private data is a basic human right that the government should take care of as a citizen's warranty. However, when the government intends to be transformed into a digital government in which all citizens' data must be associative or well-managed between each department to be analyzed, planned, and transformed into suitable policy for citizens, it can be seen that there is still no clear format to standardize data sharing method in the government sector when private data prevention in case that there is data sharing in Thailand. Therefore, it is needed to be considered with international law which can be found that there must be direct permission from the data owner before sharing or using the private data in Japan, unless there is an emergency exception related to public health, only necessary data can be used in that circumstance. Singapore has divided the private data transfer method into 2 methods, 1) measure to preserve private personal data for the citizens, and 2) measure to share the private personal data abroad. Moreover, the European Union group has divided the personal data sharing method into 2 cases which are 1) Sharing personal data with a person or a third party for a common purpose within European Union, and 2) Sharing that is related to European Union or international organization personal data transfer. Therefore, Thailand has also considered this personal data preservation format.

Keywords: Personal Data Protection Act, Data Sharing, Government Management



บทนำ

ในปัจจุบันนี้กล่าวได้ว่า มนุษย์ทุกคนเข้าสู่สังคมดิจิทัล (Digital Society) ที่เทคโนโลยีไม่เพียงเป็นเครื่องมือที่ใช้ในการติดต่อสื่อสารระหว่างกันหรือเป็นเครื่องมืออำนวยความสะดวกเท่านั้น แต่เทคโนโลยีทำให้เกิดสังคมดิจิทัลที่ส่งผลให้เกิดการหลอมรวมเทคโนโลยีเข้ากับวิถีชีวิตของมนุษย์ให้เป็นสิ่งเดียวกัน และมีลักษณะเป็นการบูรณาเทคโนโลยีขั้นสูงเข้ากับสังคมและวัฒนธรรม ส่งผลให้เกิดการเปลี่ยนโครงสร้างทางสังคมหรือเปลี่ยนแปลงรูปแบบของโครงสร้างทางเศรษฐกิจอีกต่อไปได้ (Paul, P., & Aithal, P. S., 2018) ดังนั้นเมื่อมนุษย์มีการใช้เทคโนโลยีมากยิ่งขึ้นผลที่ตามมาคือ ข้อมูลจำนวนมากในการประมวลต่าง ๆ ที่เกิดขึ้นจากการใช้เทคโนโลยี ผู้ที่มีหน้าที่ในการเก็บข้อมูลหรือสถิติต่าง ๆ อาจเป็นได้ทั้งภาครัฐและภาคเอกชน ซึ่งในการเก็บข้อมูลต่าง ๆ จากการใช้เทคโนโลยีนี้ย่อมส่งผลให้เกิดการเรียนรู้ถึงพฤติกรรมของแต่ละบุคคล เมื่อมีข้อมูลจำนวนพฤติกรรมของแต่ละบุคคลเพิ่มมากขึ้นสามารถที่จะกำหนดหรือตอบสนองต่อความต้องการของกลุ่มบุคคลได้ (Heeks, R, 2010) อย่างไรก็ตามหากใช้อย่างมีประสิทธิภาพและคำนึงถึงผลกระทบที่ตามมา เช่น การปกป้องข้อมูลของเจ้าของข้อมูลและความเป็นส่วนตัวของเจ้าของข้อมูลส่งผลให้เกิดการดำเนินงานอย่างมีประสิทธิภาพต่อองค์กรทั้งภาครัฐและภาคเอกชนเป็นอย่างมาก (De la Hoz-Rosales, et al., 2019)

หากย้อนกลับมาวิเคราะห์ถึงการบริหารหรือการดำเนินงานของรัฐบาลโดยทั่วโลกส่วนใหญ่ เรื่องการจัดการข้อมูลร่วมกันระหว่างหน่วยงานนั้นจะเห็นได้ว่า รัฐบาลส่วนใหญ่ยังไม่สามารถคว้าโอกาสในการเชื่อมโยงข้อมูลระหว่างหน่วยงานราชการด้วยกันได้ เหตุผลหลักคือการกระจายตัวของข้อมูลในลักษณะที่รับผิดชอบเฉพาะหน้าที่ในการเก็บข้อมูลของตนเองเท่านั้น ยังไม่มีการแบ่งปันข้อมูลเพื่อใช้ฐานข้อมูลเดียวกัน (Asgarkhani, M., 2005) หรือหน่วยงานมีการเก็บเป็นประจำแต่เป็นข้อมูลที่ยากต่อการประมวลผลในลักษณะที่สามารถเชื่อมโยงข้อมูล เข้าถึงข้อมูลได้อย่างมีประสิทธิภาพ (De Vries., et al., 2016) เป็นต้น ส่งผลให้การจัดการภาครัฐโดยส่วนมากเรื่องของการเชื่อมโยงข้อมูลหรือการบริหารจัดการข้อมูลของประชาชนเพื่อตอบสนองความต้องการให้แก่ประชาชนนั้นเป็นเรื่องที่ทำให้เกิดการขัดขวางการไปสู่รัฐบาลดิจิทัล (Digital Government) ได้ อีกทั้งประการหนึ่งภาคประชาชนยังขาดความเชื่อมั่นในองค์กรภาครัฐในเรื่องความโปร่งใสของข้อมูลที่หน่วยงานจัดเก็บข้อมูลส่วนบุคคลต่าง ๆ ซึ่งจะเห็นได้ว่ารัฐบาลยังไม่สร้างความไว้วางใจให้ประชาชนในการใช้ข้อมูลภาครัฐ แต่อย่างไรก็ตามจากการศึกษาของ Lwoga & Sangeda, พบว่าเมื่อรัฐบาลมีการจัดทำข้อมูลส่วนบุคคลในรูปแบบดิจิทัลที่สามารถให้หน่วยงานภาครัฐใช้ข้อมูลร่วมกันเพื่อประมวลผล ประชาชนผู้เป็นเจ้าของข้อมูลยังมีความวิตกกังวลเกี่ยวกับข้อมูลส่วนบุคคลอยู่เป็นจำนวนมากเช่น ด้านความเป็นส่วนตัว ด้านการป้องกันการละเมิดความเป็นส่วนตัว (Lwoga, E. T., & Sangeda, R. Z., 2019)

ดังนั้น การบริหารภาครัฐเพื่อให้เป็นรัฐบาลดิจิทัลที่ส่งผลต่อการใช้ประโยชน์จากข้อมูลของประชาชน ในการวิเคราะห์ตอบสนองต่อความต้องการของประชาชนนั้นจะต้องมีมาตรฐานการรักษาข้อมูลส่วนบุคคลที่เป็นรูปธรรมและส่งผลต่อการสร้างความไว้วางใจที่รัฐได้จัดทำมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน ถือได้ว่าเป็นส่วนสำคัญในการนำไปสู่รัฐบาลดิจิทัลอย่างมีประสิทธิภาพ โดยในการจัดทำมาตรฐานข้อมูลเพื่อที่จะนำไปสู่มาตรฐานที่ทั่วโลกยอมรับคือ การสร้างกรอบกฎหมายเพื่อคุ้มครองสิทธิของประชาชนและสร้างความเป็นธรรมให้แก่ประชาชน โดยในแต่ละประเทศย่อมมีกฎหมายคุ้มครองส่วนบุคคลให้แก่ประชาชนของตนเอง (Hsu, P. H., 2021) เช่น ในประเทศจีน กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Information Protection Law: PIPL (China Briefing Team, 2021) ประเทศญี่ปุ่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Act on the Protection of Personal Information: APPI (Official Gazette, 2003) ประเทศสิงคโปร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA (Chik, W. B., 2013) และ กลุ่มสหภาพยุโรป มาตราการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล หรือ General Data Protection Regulation: GDPR (Official Legal Text, 2016) เป็นต้น ส่วนของประเทศไทยนั้นมีการบัญญัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act B.E. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) เห็นได้ว่าแต่ละประเทศมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นรูปธรรมโดยการกำหนดเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมาคุ้มครองสิทธิส่วนบุคคลและความครอบคลุมความปลอดภัยให้แก่ประชาชน

ด้วยเหตุผลข้างต้น ผู้เขียนจึงต้องการเสนอกรอบคิดในการคุ้มครองข้อมูลส่วนบุคคลกรณีการแบ่งปันข้อมูลระหว่างหน่วยงานในภาครัฐ สำหรับประเทศไทยเพื่อเป็นมาตรฐานหรือแก้ไขช่องว่างทางกฎหมาย นำไปสู่การคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ พร้อมให้เกิดการบริหารแบบรัฐบาลดิจิทัล

แนวคิดการคุ้มครองข้อมูลส่วนบุคคล

สิทธิในข้อมูลส่วนบุคคล (personal data right) โดยปฎิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาติข้อ 12 บัญญัติว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัยหรือการสื่อสาร หรือจะถูกกลบหลู่เกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองของกฎหมายจากการแทรกแซงสิทธิ หรือการกลบหลู่ดังกล่าว นั้น”

ปฏิเสธไม่ได้ว่าในปัจจุบันประชาชนได้หันมาสนใจเกี่ยวกับเรื่องเทคโนโลยีมากยิ่งขึ้น ไม่ว่าจะด้วยปรากฏการณ์ของการแพร่ระบาดเชื้อโควิด-19 ส่งผลให้ประชาชนต้องมีการใช้



เทคโนโลยีมากยิ่งขึ้นเพื่อเป็นการติดต่อกับภาครัฐ อีกทั้งภาครัฐได้มีการให้บริการแก่ประชาชนในแอปพลิเคชัน (application) ที่ถือได้ว่าเป็นการอำนวยความสะดวกให้แก่ประชาชน ไม่จำเป็นต้องเดินทางมายังสถานที่ตั้งอันเป็นสำนักงานของภาครัฐ โดยภาครัฐเมื่อมีมาตรการช่วยเหลือต่าง ๆ หรือจะให้บริการข้อมูลแก่ประชาชนก็สามารถที่จะติดต่อสื่อสารได้ทางแอปพลิเคชัน สิ่งที่ตามมาเมื่อประชาชนทุกคนได้หันมาใช้เทคโนโลยีมากยิ่งขึ้นเพื่อเป็นการติดต่อกับหน่วยงานต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือภาคเอกชน สิ่งที่เพิ่มตามตัวเมื่อประชาชนใช้เทคโนโลยีเหล่านี้ในการติดต่อ คือ การเพิ่มขึ้นของข้อมูลส่วนบุคคลที่แสดงบนเว็บหรือบนแอปพลิเคชันที่เป็นการติดต่อและยืนยันตัวบุคคลในการใช้งาน เช่น ชื่อ สัญชาติ อีเมล ที่อยู่ รายละเอียดธนาคาร เป็นต้น กล่าวได้ว่าเป็นข้อมูลส่วนบุคคล

ดังนั้น เมื่อความเจริญก้าวหน้าทางเทคโนโลยีมาอย่างรวดเร็วทำให้การจัดเก็บข้อมูลการใช้ การเปิดเผย หรือการเผยแพร่ข้อมูล ถือได้ว่าเป็นข้อมูลส่วนบุคคลนั้น ได้ถูกจัดเก็บในรูปแบบต่าง ๆ แม้กระทั่งรูปแบบอิเล็กทรอนิกส์ทำให้เกิดการประมวลผลหรือเผยแพร่ข้อมูลส่วนบุคคล เพื่อให้หน่วยงานต่าง ๆ ได้บริการสาธารณะให้แก่ประชาชนได้สะดวกและรวดเร็วยิ่งขึ้น ซึ่งสิ่งที่ต้องคำนึงตามมาคือ การรักษาความปลอดภัยข้อมูลส่วนบุคคลที่หน่วยงานในภาครัฐได้นำมาวิเคราะห์ หรือใช้ข้อมูลส่วนบุคคล โดยทั่วไปแล้วข้อมูลส่วนบุคคลที่เจ้าของข้อมูลได้ให้ไว้เพื่อใช้ในการเฉพาะเรื่องเท่านั้น ไม่ได้อนุญาตให้นำไปใช้ เปิดเผย หรือเผยแพร่ในทางอื่น แต่ในความเป็นจริงแล้วข้อมูลส่วนบุคคลเหล่านั้นถูกนำไปใช้โดยปราศจากความยินยอมของเจ้าของข้อมูลซึ่งเป็นการละเมิดสิทธิส่วนบุคคลและอาจก่อให้เกิดความเดือดร้อนเสียหายแก่เจ้าของข้อมูลได้ ซึ่งปัญหาการละเมิดข้อมูลส่วนบุคคลทางนั้นสามารถเกิดขึ้นได้กับบุคคลทุกเพศทุกวัย (สุวจนี จิระวิไลกาญจน์, 2564)

แนวความคิดที่ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (personal data protection) เป็นแนวความคิดที่มีพัฒนาการมาจากการคุ้มครองสิทธิในความเป็นส่วนตัว (privacy right) มีพัฒนาการมาเป็นระยะเวลายาวนานแล้วโดยตั้งแต่ในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องความเป็นส่วนตัวยอมรับว่าบุคคล แต่ละคนมีเขตแดนของตนเอง ในเขตแดนเสมือนเป็นที่พักที่บุคคลไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาส่วนตัว เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องจากคนอื่น (นคร เสรีรักษ์, 2557) แนวความคิดในการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจนและได้รับการยอมรับมากที่สุดเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” หรือ “สิทธิในความเป็นส่วนตัว” ของ Samuel & Louis (1890) ที่สะท้อนปัญหาการคุกคามความเป็นส่วนตัวของปัจเจกบุคคลจากการนำเสนอข่าวของสื่อมวลชน ผู้เขียนอธิบายว่าสิทธิในความเป็นส่วนตัวหมายถึง สิทธิที่จะอยู่โดยลำพัง (right to be let alone) โดยได้รับอิสระปราศจากการครอบงำจากบุคคลอื่นหรือผู้ปกครอง

หลักการคุ้มครองข้อมูลส่วนบุคคลส่วนบุคคลในปัจจุบัน ได้มีการกำหนดไว้ใน General Data Protection Regulation มาตรา 5 ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งถือได้ว่าเป็นบรรทัดฐานในการคุ้มครองข้อมูลส่วนบุคคล จะต้องประกอบด้วย

ประการที่หนึ่ง ความถูกต้องตามกฎหมาย เป็นธรรม และความโปร่งใส (Lawfulness, fairness, and transparency): การประมวลผลข้อมูลส่วนบุคคลใด ๆ ควรถูกกฎหมายและยุติธรรม พร้อมทั้งมีความโปร่งใสต่อบุคคลที่มีการรวบรวม ใช้ข้อมูล หรือประมวลผลข้อมูลส่วนบุคคลที่ หลักการของความโปร่งใสกำหนดให้ข้อมูลและการสื่อสารใด ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลเหล่านั้นสามารถเข้าถึงได้ง่ายและเข้าใจได้ง่าย และใช้ภาษาที่ชัดเจน

ประการที่สอง รวบรวมเพื่อวัตถุประสงค์ที่เฉพาะ (Purpose Limitation) ข้อมูลส่วนบุคคลควรถูกรวบรวมเพื่อวัตถุประสงค์ที่ระบุ ชัดเจน และชอบด้วยกฎหมายด้วยกฎหมายเท่านั้น และไม่ควรประมวลผลเพิ่มเติมในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้น โดยเฉพาะอย่างยิ่ง วัตถุประสงค์เฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลควรมีความชัดเจนและถูกต้องตามกฎหมาย

ประการที่สาม การลดขนาดข้อมูล (Data Minimisation) การประมวลผลข้อมูลส่วนบุคคลต้องเพียงพอ มีความเกี่ยวข้อง และจำกัดเฉพาะสิ่งที่จำเป็นที่เกี่ยวข้องกับวัตถุประสงค์ในการประมวลผล ข้อมูลส่วนบุคคลควรได้รับการประมวลผลเฉพาะในกรณีวัตถุประสงค์ของการประมวลผล

ประการที่สี่ ความถูกต้อง (Accuracy) ผู้ควบคุมต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกต้องและไม่ประมวลผลนอกเหนือไปจากที่ตกลงไว้แต่ต้นด้วยวิธีการที่เข้ากับวัตถุประสงค์ไม่ได้

ประการที่ห้า ข้อจำกัดในการจัดเก็บ (Storage Limitation) ข้อมูลส่วนบุคคลควรเก็บไว้ในรูปแบบที่อนุญาตให้ระบุเจ้าของข้อมูลได้ทราบเท่าที่จำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลจะไม่ถูกเก็บไว้นานเกินความจำเป็น

ประการที่หก ความสมบูรณ์และการรักษาความลับ (Integrity and Confidentiality) ข้อมูลส่วนบุคคลควรได้รับการประมวลผลในลักษณะที่รับรองความปลอดภัยที่เหมาะสมและความลับของข้อมูลส่วนบุคคลรวมถึงการป้องกันการเข้าถึงหรือการใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือผิดกฎหมาย

ประการที่เจ็ด ความรับผิดชอบ (Accountability) ผู้ควบคุมมีหน้าที่และต้องสามารถแสดงให้เห็นได้ว่าได้ปฏิบัติตามหลักการในการปกป้องข้อมูลที่มีชื่อข้างต้นทั้งหมด ผู้ควบคุมต้องรับผิดชอบต่อผลการประมวลผลข้อมูลส่วนบุคคลและวิธีปฏิบัติตาม GDPR ที่ได้มีการกำหนดไว้



ดังนั้น จะเห็นได้ว่าข้อมูลส่วนบุคคลของประชาชน ถือได้ว่าเป็นส่วนหนึ่งของสิทธิขั้นพื้นฐานที่รัฐบาลควรที่จะให้ความคุ้มครองและมีมาตรการในการคุ้มครอง อีกทั้งการบริหารภาครัฐในปัจจุบันก็ต้องมีการใช้ข้อมูลส่วนบุคคลของประชาชนในการวิเคราะห์ กำหนดนโยบายต่าง ๆ เพื่อให้ประชาชนอย่างมีประสิทธิภาพและประสิทธิผล หากรัฐบาลไม่สามารถคุ้มครองข้อมูลส่วนบุคคลของประชาชนได้อย่างมีประสิทธิภาพ อาทิ ข้อมูลรั่วไหล มีการระบบการป้องกันข้อมูลที่ไม่เพียงพอ หรือมีการขายข้อมูลส่วนบุคคลให้แก่บุคคลอื่น ย่อมถือได้ว่ารัฐเองกำลังกระทำการละเมิดสิทธิส่วนบุคคลของประชาชน ดังนั้นรัฐบาลควรที่จะมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐในการบริหาร

มาตรการการคุ้มครองข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐในการบริหาร

การศึกษามาตรการการคุ้มครองข้อมูลส่วนบุคคลในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐในการบริหาร เป็นการศึกษาเพื่อหาแนวทางในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนเพื่อที่จะก่อให้เกิดความคุ้มครองและความปลอดภัย โดยเป็นการศึกษาเปรียบเทียบ ประเทศไทย และต่างประเทศ เพื่อหารูปแบบการคุ้มครองที่เหมาะสม

1. การคุ้มครองข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลในประเทศไทย ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐในการบริหาร

ประเทศไทยในการมุ่งหมายเพื่อให้เป็นรัฐบาลดิจิทัล ได้มีการบัญญัติพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีเหตุผลเนื่องปัจจุบันเทคโนโลยีได้มีความก้าวหน้าและเป็นส่วนหนึ่งในวิถีชีวิตและการประกอบธุรกิจของประชาชน ซึ่งในการบริหารงานและการให้บริการภาครัฐที่ผ่านมายังมีได้นำเทคโนโลยีมาใช้ในการพัฒนาให้เกิดประสิทธิภาพและอำนวยความสะดวกแก่ประชาชนได้อย่างเต็มที่ และโดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้มีการปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน โดยให้มีการนำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้ในการบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะ และให้มีการบูรณาการฐานข้อมูลของหน่วยงานของรัฐทุกหน่วยงานเข้าด้วยกันเพื่อให้เป็นระบบข้อมูล เพื่อประโยชน์ในการบริหารราชการแผ่นดินและเพื่ออำนวยความสะดวกให้แก่ประชาชน สมควรให้มีกฎหมายในการขับเคลื่อนให้เกิดการปฏิรูปการบริหารราชการแผ่นดินและการบริการประชาชนตามบทบัญญัติแห่งรัฐธรรมนูญ และเพื่อยกระดับการบริหารงานและการให้บริการภาครัฐให้อยู่ในระบบดิจิทัล อันจะนำไปสู่การเป็นรัฐบาลดิจิทัลที่มีระบบการทำงานและข้อมูลเชื่อมโยงกันระหว่างหน่วยงานของรัฐอย่างมั่นคงปลอดภัย มีประสิทธิภาพ รวดเร็ว เปิดเผยและโปร่งใส รวมทั้งประชาชนได้รับความสะดวกใน

การรับบริการและสามารถตรวจสอบการดำเนินงานของหน่วยงานของรัฐได้ จึงจำเป็นต้องตราพระราชบัญญัตินี้ จึงเห็นได้ว่าตั้งแต่ปี พ.ศ. 2562 รัฐต้องการจะผลักดันให้องค์กรภาครัฐมีรูปแบบการบริหารงานดิจิทัล

อย่างไรก็ตามเมื่อรัฐบาลต้องการให้หน่วยงานมีการบริหารหรือตอบสนองต่อความต้องการของประชาชน ในการใช้ประโยชน์ร่วมกันในข้อมูลระหว่างหน่วยงานจึงได้มีการบัญญัติไว้ในมาตรา 13 ของพระราชบัญญัตินี้ดังกล่าว โดยบัญญัติว่า “เพื่อประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอ ที่จะเกิดการบูรณาการร่วมกัน” ดังนั้นจะเห็นได้ว่าตั้งแต่ปี พ.ศ. 2562 รัฐบาลของประเทศไทยได้มีนโยบายที่ให้หน่วยงานภาครัฐสามารถมีการแบ่งปันข้อมูลส่วนบุคคลเพื่อตอบสนองต่อการจัดการและบริการประชาชนได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น แต่อย่างไรก็ตามจะเห็นได้ว่าในพระราชบัญญัตินี้ไม่ได้มีการกำหนดมาตรฐานการแบ่งปันข้อมูลส่วนบุคคลของหน่วยงานภาครัฐ การรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประชาชน และการกำหนดโทษ มีเพียงการกำหนดมาตรฐานขั้นพื้นฐานรักษาข้อมูลส่วนบุคคล จึงจำเป็นต้องใช้กฎหมายในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาประกอบการพิจารณาในการวิเคราะห์เพื่อกำหนดรูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป (สำนักงานคณะกรรมการกฤษฎีกา, 2562) ส่งผลให้ในปัจจุบันประเทศไทยได้มีการบัญญัติถึงการคุ้มครองข้อมูลส่วนบุคคล โดยได้มีการนิยาม “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อีกทั้งเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

การกำหนดโทษในตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โทษตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากมีผู้กระทำการฝ่าฝืนสามารถได้รับ



โทษด้วยกัน 3 ทางกล่าวคือ โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง ซึ่งสามารถอธิบายได้ดังนี้

โทษความรับผิดทางแพ่ง มาตรา 78 ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

โทษความรับผิดอาญา มาตรา 79 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืน โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ และในมาตรา 80 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

โทษความรับผิดทางปกครอง เช่น มาตรา 82 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติ..... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท มาตรา 85 ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติ... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท และมาตรา 88 ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตาม... ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท เป็นต้น

ซึ่งจะเห็นได้ว่าการคุ้มครองข้อมูลส่วนบุคคลของประชาชนนั้น ถึงแม้จะได้มีมาตรการลงโทษถึง 3 สถานด้วยกัน แต่ในขอบเขตเรื่องการแบ่งปันข้อมูลส่วนบุคคลสำหรับมาตรฐานในประเทศไทย ยังถือได้ว่ายังไม่มียกเว้นที่เฉพาะในการคุ้มครองข้อมูลส่วนบุคคลกรณีของการแบ่งปันข้อมูลส่วนบุคคล หากเกิดกรณีที่หน่วยงานภาครัฐเกิดการใช้ข้อมูลส่วนบุคคลไปในทางที่ผิดหรือทำให้เกิดความเสียหาย อาจส่งผลกระทบต่อความเชื่อมั่นของประชาชนในการบริหารประเทศที่จะเกิดขึ้นในอนาคตได้ ดังนั้นจึงนำมาสู่การศึกษาเปรียบเทียบการการคุ้มครองข้อมูลส่วนบุคคลกรณีของการแบ่งปันข้อมูลส่วนบุคคลของต่างประเทศว่ามีรูปแบบหรือมาตรการในการป้องกันอย่างไรในการจัดทำนโยบายที่เกิดขึ้น

2. มุมมองกฎหมายการแบ่งปันข้อมูลส่วนบุคคลในต่างประเทศ ประเทศญี่ปุ่น

ได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) เริ่มมีผลบังคับใช้ในปี พ.ศ. 2548 ซึ่งเป็นการเปลี่ยนแปลงครั้งสำคัญในวิธีการปกป้องข้อมูลส่วนบุคคล เดิมทีผู้ประกอบการเอกชนหรือภาครัฐ หากได้มีการกระทำการข้อมูลส่วนบุคคลของบุคคลอื่นให้เกิดความเสียหาย บุคคลผู้ได้รับความเสียหายจะขอชดเชยค่าเสียหายตามจะต้องครบองค์ประกอบความผิดตามกฎหมายละเมิด แต่เมื่อมีการบัญญัติถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้วนั้น จึงต้องมาใช้พระราชบัญญัตินี้ดังกล่าวแทน (Miyashita, H., 2011) การกำหนดว่าการถ่ายโอนข้อมูลโดยทั่วไปแล้วการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม เป็นกรณีที่เจ้าของข้อมูลไม่ได้รับความยินยอมล่วงหน้าจากหน่วยงานจะไม่สามารถกระทำได้ เว้นแต่จะมีข้อยกเว้น:

1. การโอนที่ได้รับอนุญาตตามกฎหมาย หากเป็นกรณีที่ได้รับอนุญาตแล้วไม่จำเป็นต้องได้รับความยินยอมล่วงหน้าจากเจ้าของหลักในการถ่ายโอนข้อมูลส่วนบุคคล (รวมถึงข้อมูลที่มีลักษณะละเอียดอ่อน)

2. กรณีที่ต้องได้รับความยินยอมจากเจ้าของข้อมูล ที่ถือว่าเป็นข้อกำหนดหรือได้รับอนุญาตโดยเฉพาะตามกฎหมายหรือข้อบังคับของญี่ปุ่น จะต้องเป็นกรณีที่มีความจำเป็นสำหรับการปกป้องชีวิต สุขภาพ หรือทรัพย์สินของบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลเป็นการยากเท่าที่จำเป็น

3. มีความจำเป็นสำหรับการพัฒนาด้านสาธารณสุขและสุขอนามัย หรือการส่งเสริมการเลี้ยงดูที่ดี และการได้รับความยินยอมจากผู้ปกครองหรือบิดา มารดา นั้นทำได้ยาก เท่าที่จำเป็น

ซึ่งจะเห็นได้ว่าสำหรับกฎหมายในเรื่องการแบ่งปันข้อมูลส่วนบุคคลในประเทศญี่ปุ่นนั้น ถือได้ว่ามีหลักการคือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อน แต่อย่างไรก็ตามหากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถานการณ์นั้นที่เกิดขึ้น

ประเทศสิงคโปร์

การบัญญัติกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) ในมาตรา 26 ของ PDPA โดยมีการกำหนด โดยจำกัดองค์กรต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชนไม่ให้ถ่ายโอนข้อมูลส่วนบุคคลออกนอกประเทศสิงคโปร์ หรือเรียกอีกอย่างหนึ่งว่า ข้อผูกพันในการจำกัดการโอน (Transfer Limitation obligation) เว้นแต่จะมีการป้องกันที่กำหนดไว้อย่างน้อยหนึ่งอย่าง



เพื่อให้แน่ใจว่าผู้รับข้อมูลจะให้มาตรฐานการป้องกันการถ่ายโอน ข้อมูลส่วนบุคคลที่เทียบเท่ากับการคุ้มครองภายใต้ PDPA ข้อบังคับยังระบุขั้นตอนที่องค์กรอาจดำเนินการเพื่อให้แน่ใจว่าผู้รับข้อมูลส่วนบุคคลในต่างประเทศจะต้องถูกผูกมัดที่จะต้องบังคับตามกฎหมายเพื่อให้มีมาตรฐานการป้องกันข้อมูลส่วนบุคคลที่เทียบเท่ากับข้อมูลส่วนบุคคลที่ถ่ายโอนไป

ทั้งนี้ ในพระราชบัญญัติได้มีการกำหนดกลไกและวิธีการการถ่ายโอนข้อมูลส่วนบุคคลที่เกิดขึ้นภายในประเทศจะต้องมีองค์ประกอบที่รวมถึง 1. มีความยินยอมจากเจ้าของของข้อมูลของแต่ละบุคคล โดยมีเงื่อนไขว่าได้ดำเนินการตามขั้นตอนที่กำหนดไว้ในกาได้รับความยินยอมดังกล่าว 2 จะต้องมิขัดแย้งที่มีผลผูกพันทางกฎหมายเพื่อกำหนดภาระหน้าที่ในการปกป้องข้อมูลให้กับเจ้าของข้อมูลส่วนบุคคล 3. การถ่ายโอนข้อมูลจะต้องทำตามสัญญาที่ได้ตกลงกันไว้ (Singapore Statutes Online, 2022)

ดังนั้น ในการกำหนดวิธีการแบ่งปันข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้แบ่งวิธีการโอนข้อมูลส่วนบุคคลออกเป็น 2 ลักษณะ คือ 1. มาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ 2. มาตรการแบ่งปันข้อมูลส่วนบุคคลให้กับต่างประเทศ ซึ่งหลักการสำคัญของทั้ง 2 มาตรการในการแบ่งปันข้อมูลส่วนบุคคลทั้ง 2 วิธี คือจะต้องมีการขอความยินยอมหรืออนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะสามารถทำการแบ่งปันข้อมูลส่วนบุคคลได้

กลุ่มสหภาพยุโรป

สหภาพยุโรปได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ General Data Protection Regulation : GDPR ซึ่งจะมีผลบังคับใช้ในวันที่ 25 พฤษภาคม 2561 ซึ่งถือได้ว่าเป็นกฎหมายที่เป็นสาระสำคัญสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่พลเมืองสหภาพยุโรปและบริษัทต่าง ๆ ประกอบกิจการในสหภาพยุโรปจะต้องปฏิบัติตาม ทั้งนี้ในส่วนของการแบ่งปันข้อมูลส่วนบุคคลกฎหมาย GDPR ของสหราชอาณาจักรกำหนดข้อจำกัดและเงื่อนไขบางประการในการแบ่งปันข้อมูลส่วนบุคคลกับองค์กรหรือหน่วยงานให้แก่บุคคลที่สาม เพื่อก่อให้เกิดความแน่ใจว่าข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเหมาะสมและจัดการโดยผู้อื่นอย่างเหมาะสม อีกทั้งเป็นหลักประกันในทางกฎหมายและความโปร่งใสสำหรับผู้ปฏิบัติงาน ให้มีมาตรฐานการทำงานอย่างเป็นระบบ และเท่าเทียมกันเป็นมาตรฐาน (Voigt, P., & Von dem Bussche, A., 2017) จึงได้มีการกำหนดการแบ่งปันข้อมูลแบ่งออกเป็น 2 ประเภท กล่าวคือ

ประเภทที่ 1 การแบ่งปันข้อมูลส่วนบุคคลกับบุคคลหรือหน่วยงานที่สามเพื่อใช้ในวัตถุประสงค์ร่วมกันภายในสหภาพยุโรป ซึ่งมีการบัญญัติไว้ในหมวด 2: เรื่องการแบ่งปันข้อมูลส่วนบุคคลไปยังบุคคลที่สามเพื่อใช้ตามวัตถุประสงค์ของตนเอง โดยให้มีการกำหนดมาตรฐานการจัดเก็บข้อมูล ทั้งนี้ในการเคลื่อนย้ายข้อมูลส่วนบุคคลเพื่อแบ่งปันนั้นจะต้องมีทำหนังสือบอกกล่าวการบอกกล่าวถึงวัตถุประสงค์ของการเคลื่อนย้ายข้อมูลเพื่อให้เจ้าของข้อมูลส่วนบุคคลรับรู้ตั้งแต่ต้นของการแบ่งปันข้อมูล อีกทั้งจะต้องมีการกำหนดขอบเขตของการวิเคราะห์

ข้อมูลอย่างชัดเจน และให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อสำหรับเจ้าหน้าที่ หากต้องการแสดงความยินยอมในการติดแบ่งปันข้อมูลได้ทุกเมื่อ

ประเภทที่ 2 การแบ่งปันที่เกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนบุคคลสหภาพยุโรปหรือองค์การระหว่างประเทศ โดยมีการกำหนดให้ผู้ควบคุมหรือผู้ประมวลผลข้อมูลจะต้องมีการปฏิบัติตามกฎหมายฉบับนี้ เพื่อเป็นหลักประกันการให้แก่เจ้าของข้อมูลส่วนบุคคลไม่ถูกล่วงละเมิดในข้อมูลส่วนบุคคล โดยมีหลักในการปฏิบัติตาม บรรพ 5 การเคลื่อนย้ายข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศ ดังนี้

1. ให้หน่วยงานหรือองค์กรต้นทางพิจารณาความเสี่ยงของการโอนข้อมูลส่วนบุคคลหรือเรียกว่าการ “ประเมินความเสี่ยง” ข้อมูลส่วนบุคคลจะได้รับการดูแลในองค์กรที่จะถูกโอนไป อยู่ในประเทศที่มีกฎหมายคุ้มครองข้อมูลในระดับที่เหมาะสมและการใช้ทางกฎหมายสำหรับบุคคลหรือไม่?

2. ขอให้องค์กรหรือหน่วยงานที่สามลงนามใน Standard Contractual Clauses สำหรับการโอนโดยจะต้องไม่ทำการแก้ไขใด ๆ โดยเป็นส่วนหนึ่งของเอกสารสัญญา

- 3 การแบ่งปันข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน พร้อมทั้งจะต้องมีการระบุถึงรายละเอียดของการแบ่งปันข้อมูลส่วนบุคคลเพื่อที่จะไปใช้ พร้อมทั้งมีการกำหนดระยะเวลาในการขอความยินยอมการใช้ข้อมูลส่วนบุคคลจากเจ้าของข้อมูลอย่างชัดเจน

4. หน่วยงานหรือองค์กรต่างประเทศหน่วยงานที่สาม จะต้องมีการปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานกฎหมายฉบับนี้ อีกทั้งมีผลผูกพันในทางกฎหมายและสามารถถูกลงโทษได้ตามกฎหมายฉบับนี้เช่นเดียวกัน

5. เมื่อมีการใช้ข้อมูลเสร็จแล้วจะต้องมีการทำลายหรือมีการส่งกลับข้อมูลส่วนบุคคลแล้วแต่ตามที่ตกลงกัน เพื่อให้เป็นหลังประกันว่า

เห็นได้ว่า การแบ่งปันข้อมูลส่วนบุคคลสำหรับกลุ่มสหภาพยุโรปได้แบ่งรูปแบบการแบ่งปันข้อมูลส่วนบุคคลออกเป็น 2 กรณีกล่าวคือ 1. การแบ่งปันข้อมูลส่วนบุคคลกับบุคคลหรือหน่วยงานที่สามเพื่อใช้ในวัตถุประสงค์ร่วมกันภายในสหภาพยุโรป 2 การแบ่งปันที่เกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนบุคคลสหภาพยุโรปหรือองค์การระหว่างประเทศ ซึ่งรูปแบบการคุ้มครองข้อมูลส่วนบุคคล

สรุป

การนำไปสู่รัฐบาลดิจิทัล (Digital Government) เพื่อการวิเคราะห์ข้อมูลและวางแผนต่าง ๆ นโยบาย โดยการใช้ประโยชน์จากข้อมูลของประชาชนในการวิเคราะห์ตอบสนองต่อความต้องการของประชาชนนั้นจะต้องมีมาตรฐานการรักษาข้อมูลส่วนบุคคลที่เป็นรูปธรรมและ



ส่งผลต่อการสร้างความไว้วางใจที่รัฐได้จัดทำมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน ถือได้ว่าเป็นส่วนสำคัญในการนำไปสู่รัฐบาลดิจิทัลอย่างมีประสิทธิภาพ ซึ่งการคุ้มครองข้อมูลส่วนบุคคล ถือเป็นสิทธิมนุษยชนขั้นพื้นฐาน (fundamental human rights) ที่จะต้องได้รับการเคารพจากบุคคลอื่น เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะปกป้องข้อมูลของตน หลักดังกล่าวเป็นที่ยอมรับกันในระดับนานาชาติทุกประเทศในโลกต่างให้ความสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก เมื่อพิจารณากฎหมายการแบ่งปันข้อมูลส่วนบุคคลในต่างประเทศ ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐในการบริหาร ใน**ประเทศญี่ปุ่น** การแบ่งปันข้อมูลส่วนบุคคลในประเทศญี่ปุ่นนั้น ถือได้ว่ามีหลักการคือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อนที่จะมีการแบ่งข้อมูลส่วนบุคคล หรือก่อนที่มีการใช้ข้อมูลส่วนบุคคลได้จะต้องยินยอม เว้นแต่มีข้อยกเว้นหากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถานการณ์นั้นที่เกิดขึ้น **ประเทศสิงคโปร์**ได้แบ่งวิธีการโอนข้อมูลส่วนบุคคลออกเป็น 2 ลักษณะ คือ 1. มาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ 2. มาตรการแบ่งปันข้อมูลส่วนบุคคลให้กับต่างประเทศ ซึ่งหลักการสำคัญของทั้ง 2 มาตรการในการแบ่งปันข้อมูลส่วนบุคคลทั้ง 2 วิธี คือจะต้องมีการขอความยินยอมหรืออนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะสามารถทำการแบ่งปันข้อมูลส่วนบุคคลได้ **กลุ่มสหภาพยุโรป**ได้แบ่งรูปแบบการแบ่งปันข้อมูลส่วนบุคคลออกเป็น 2 กรณีกล่าวคือ 1. การแบ่งปันข้อมูลส่วนบุคคลกับบุคคลหรือหน่วยงานที่สามเพื่อใช้ในวัตถุประสงค์ร่วมกันภายในสหภาพยุโรป 2 การแบ่งปันที่เกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนบุคคลสหภาพยุโรปหรือองค์การระหว่างประเทศ ซึ่งส่งผลให้เกิดรูปแบบการคุ้มครองข้อมูลส่วนบุคคล

เอกสารอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. (2562). ราชกิจจานุเบกษา เล่ม 136 ตอน 69 ก. หน้า 52- 95 (27 พฤษภาคม 2562).
- สำนักงานคณะกรรมการกฤษฎีกา. (2562). มาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป. เรียกใช้เมื่อ 29 พฤษภาคม 2565 จาก <https://www.krisdika.go.th/th/home>
- สุวจนี จิระวิไลกาญจน์. (2564). การตระหนักรู้เกี่ยวกับการปกป้องสิทธิส่วนบุคคล จากการใช้ข้อมูลส่วนบุคคลในภาครัฐกิจของประชาชนในกรุงเทพมหานคร. วารสารนิติศาสตร์ปริทัศน์, 25(3), 35-53.
- Asgarkhani, M. (2005). Digital government and its effectiveness in public management reform: A local government perspective. Public Management Review, 7(3), 465-487.

- Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, 29(5), 554-575.
- China Briefing Team. (2021). The PRC Personal Information Protection Law. Retrieved May 29, 2022, from <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>
- De la Hoz-Rosales, et al. (2019). Effects of information and communication technology usage by individuals, businesses, and government on human development: An international analysis. *IEEE Access*, 7(4), 129225-129243.
- De Vries., et al., (2016). Innovation in the public sector: A systematic review and future research agenda. *Public administration*, 94(1), 146-166.
- Heeks, R. (2010). Do information and communication technologies (ICTs) contribute to development ? *Journal of international development*, 22(5), 625-640.
- Hsu, P. H. (2021). Emerging China Data Protection Law: Soft Power from EU GDPR? *Tamkang Journal of International Affairs*, 25(1), 287-310.
- Lwoga, E. T., & Sangeda, R. Z. (2019). ICTs and development in developing countries: A systematic review of reviews. *The Electronic Journal of Information Systems in Developing Countries*, 85(1), 1-17.
- Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. *International Data Privacy Law*, 1(4), 229-238.
- Official Gazette. (2003). Act on the Protection of Personal Information. Retrieved May 29, 2022, from <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>
- Official Legal Text. (2016). General Data Protection Regulation. Retrieved May 29, 2022, from <https://gdpr-info.eu/>
- Paul, P., & Aithal, P. S. (2018). Digital Society: Its Foundation and Towards an Interdisciplinary Field. *SIMS Pandeshwar & Srinivas University Mukka*, 3(12), 1-6.
- Singapore Statutes Online. (2022). PERSONAL DATA PROTECTION ACT 2012. Retrieved April 10, 2022, from <https://sso.agc.gov.sg/Act/PDPA2012>
- Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st Ed., Cham. Springer International Publishing, Switzerland.