หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

Personal Data Protection Principles: Comparative study of the Personal Data Protection Act, B.E. 2562 and the Official Information Act, B.E. 2540

นพดล นิ่มหนู[1]
Noppadon Nimnoo[1]

Recived: 27th July 2021 **Revised**: 21st September 2021 **Accept**: 12th October 2021

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะอย่างยิ่งตามกฎหมายสองฉบับคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ว่ามีมาตรฐานในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานสากลหรือไม่ โดยใช้การดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) ในรูปแบบการวิจัยเอกสาร (Documentary Research) ผลการศึกษาพบว่าหลักการคุ้มครองข้อมูลส่วนบุคคลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีฐานะเป็นกฎหมายกลาง กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิตินั้นได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ แต่สำหรับในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ มุ่งเน้นคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานภาครัฐ ยังมีประเด็นปัญหาเกี่ยวกับหลักการคุ้มครองข้อมูลอยู่หลายประการ ไม่ว่าจะเป็นเรื่องของการเก็บรักษาข้อมูล การกำหนดให้มีเจ้าหน้าที่ควบคุมข้อมูล การประมวลผลและการใช้ข้อมูลส่วนบุคคล ซึ่งมาตรฐานยังแตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผู้วิจัยจึงเสนอให้มีการทำการทบทวนหลักการและแก้ไขบทบัญญัติ เพื่อให้กฎหมายทั้งสองฉบับมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลเป็นไปในทิศทางเดียวกันโดยไม่เกิดภาวะสองมาตรฐาน

คำสำคัญ: ข้อมูลข่าวสารของราชการ, สิทธิในข้อมูลส่วนบุคคล, การคุ้มครองข้อมูลส่วนบุคคล

[1] อาจารย์ประจำ, คณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม

[1] Lecturer, Faculty of Law, Mahasarakham university

Abstract

The purpose of this research was to compare the principles of personal data protection in Thailand. In particular, according to two laws, namely the Personal Data Protection Act B.E. 2562 (2019) and the Government Information Act B.E. by using qualitative research in the form of documentary research. Personal Data Protection Principles of the Personal Data Protection Act B.E. 2562 is the central law determining the principles of personal data protection in a general manner and covering all dimensions. It is influenced by the European Union Personal Data Protection Act (GDPR), it provides standards for the protection of rights equal to those of other civilized countries. However, the Government Information Act, BE 2540 (1997), contains a specific principle for personal data protection. The focus is on protecting personal data that is in the control of government agencies. There are still a number of issues with data protection principles. whether it is a matter of data retention, assigning a data control officer, processing and use of personal data The standards are still different from the Personal Data Protection Act B.E. 2562, therefore, the researcher proposes to review the principles and amend the provisions to ensure that the two laws have the same standards of personal data protection.

Keywords: Public Information, rights to information, data protection.

บทนำ

ข้อมูลส่วนบุคคลนั้น มีสถานะเป็นทั้งทรัพย์สินส่วนตัวของบุคคลและขณะเดียวกัน ก็เป็นสิทธิในความเป็นอยู่ส่วนตัวของบุคคลอันเป็นสิทธิมนุษยชนขั้นพื้นฐาน การล่วงละเมิดข้อมูลส่วนบุคคลจึงเป็นการล่วงละเมิดในทรัพย์สินของบุคคลและเป็นการล่วงละเมิดสิทธิส่วนบุคคลไปในขณะเดียวกัน โดยเฉพาะอย่างยิ่งในยุคที่นานาอารยะประเทศมีพลวัตรทางเทคโนโลยีอย่างสูง ทำให้การล่วงละเมิดข้อมูลส่วนบุคคลนั้น เกิดขึ้นได้โดยง่าย ไม่ว่าโดยการกระทำของเอกชนด้วยกัน หรือโดยการกระทำของฝ่ายรัฐเอง ไม่ว่าจะเป็นการเก็บรวมรวมข้อมูล การนำข้อมูลส่วนบุคคลไปใช้ประมวลผล หรือเปิดเผย หรือกระทำการใดๆ ที่ทำให้เจ้าของข้อมูลส่วนบุคคลต้องได้รับความ เสียหาย ไม่ว่าจะเป็นด้านความปลอดภัยต่อชีวิตร่างกาย สิทธิเสรีภาพ หรือการเอาข้อมูลไปใช้ประโยชน์ทางธุรกิจโดยไม่ได้รับอนุญาตอันเป็นการสร้างความเดือนร้อนรำคาญแก่เจ้าของข้อมูล เป็นต้น เมื่อพิจารณาจากสถิติการล่วงละเมิดข้อมูลส่วนบุคคลของประเทศสหรัฐอมริกา ในปี พศ.2563 (ค.ศ.2020) จำนวนการละเมิดข้อมูลส่วนบุคคลมีทั้งหมด 1001 คดี โดยมีประชาชนกว่า 155.8 ล้านคนได้รับผลกระทบจากการละเมิดเช่นนี้ ซึ่งแนวโน้มการละเมิดนี้เพิ่มขึ้นมาตลอดนับแต่ปี 2005 จนถึงมากที่สุดในปี 2017 แต่อัตราการละเมิดอยู่ในภาพรวมที่มีแนวโน้มจะสูงขึ้น (Johnson, 2021) โดยนอกจากกรณีนี้ยังมีสถานการณ์การละเมิดทำนองเดียวกันเกิดขึ้นทุกมุมของโลก เป็นเหตุทำให้นานาอารยะประเทศตระหนักถึงปัญหาที่เกิดขึ้น และพยายามสร้างมาตรการต่างๆ อันเป็นหลักการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาตั้งแต่อดีตจนปัจจุบัน โดยเฉพาะอย่างยิ่ง กลุ่มประเทศสหภาพยุโรป ได้พัฒนาหลักการที่เรียกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection

Regulation ขึ้นมา ซึ่งมีอิทธิพลอย่างสูงต่อหลักการคุ้มครองข้อมูลส่วนบุคคลของทุกประเทศทั่วโลก รวมถึงประเทศไทยที่เป็นประเทศคู่ค้าอีกประเทศหนึ่งของสหภาพยุโรปที่จะต้องพัฒนาหลักการคุ้มครองข้อมูลส่วนบุคคลนี้ให้มีมาตรฐานเช่นเดียวกัน

สำหรับหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในปัจจุบัน รัฐสภาได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ออกมา โดยมีเนื้อหาสาระเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิในความเป็นส่วนตัว ซึ่งมีที่มาการเสนอร่างกฎหมายดังกล่าวในเดือนพฤษภาคม พ.ศ.2558 โดยได้รับอิทธิพลมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation นั่นเอง โดยลักษณะการตรานั้น เป็นการกำหนดให้กฎหมายฉบับนี้ เป็นกฎหมายกลางที่กำหนด หลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล เป็นไปตามมาตรฐานสากล และมีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิด รวมทั้งมีการการกำหนดโทษปรับทางปกครอง ความรับผิดทางแพ่งและทางอาญาค่อนข้างสูงมากเมื่อเทียบกับกฎหมายฉบับอื่นๆ ทั้งนี้เพื่อให้หลักการคุ้มครองข้อมูลส่วนบุคคลสามารถสัมฤทธิ์ผลได้ในทางปฏิบัติ แต่อย่างไรก็ดี ในระบบกฎหมายของประเทศไทย ยังมีหลักการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ตามกฎหมายเฉพาะต่างๆ อีกหลายฉบับ โดยเฉพาะอย่างยิ่ง พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งกำหนดหลักการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ที่อยู่ในความครอบครอง ควบคุมดูแลโดยภาครัฐนั้นเอง ดังนั้น จึงกล่าวได้ว่า ข้อมูลส่วนบุคคลที่อยู่กับภาครัฐ โดยเฉพาะอย่างยิ่งหน่วยงานของรัฐซึ่งทำหน้าที่เป็นผู้เก็บรวบรวม ใช้ ประมวลผล เปิดเผยนั้น หาได้ตกอยู่ภายใต้บังคับของกฎหมายกลางที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลแต่อย่างใด ทำให้เกิดประเด็นว่า ข้อมูลส่วนบุคคลที่อยู่กับภาคเอกชน อยู่ภายใต้หลักการคุ้มครองข้อมูลตามพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ.2562 แต่ ข้อมูลส่วนบุคคลที่อยู่กับภาครัฐ อยู่ภายใต้หลักการคุ้มครองข้อมูลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

ประเด็นจึงน่าสนใจที่จะศึกษาว่า หลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของประเทศไทย โดยเฉพาะกฎหมายกลางซึ่งก็คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในภาพรวม และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่กำหนดหลักการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่กับภาครัฐ ว่าจะมีความเหมือนหรือแตกต่างกันอย่างไร และเราจะพัฒนาหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายทั้งสองฉบับให้สอดคล้องกับหลักการสากลและเป็นไปโดยมีมาตรฐานที่ไม่ได้แตกต่างกัน

ความมุ่งหมายของการวิจัย

1. เพื่อศึกษาแนวความคิด ทฤษฎี และหลักการคุ้มครองข้อมูลส่วนบุคคลตามกติกาสากลและกฎหมายของต่างประเทศที่สำคัญ

2. เพื่อเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

3. เพื่อเสนอแนวทางพัฒนาหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายทั้งสองฉบับให้เป็นไปในทิศทางเดียวกันและมีมาตรฐานทัดเทียมกับหลักการของต่างประเทศ

วิธีวิจัย

การศึกษาวิจัยเกี่ยวกับเรื่องนี้จะใช้การดำเนินการวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้รูปแบบการวิจัยเอกสาร (Documentary Research) เช่นตำราวิชาการ หนังสือ รายงานการวิจัย วิทยานิพนธ์ตลอดจนเอกสารจากฐานข้อมูลออนไลน์ทั้งในและต่างประเทศ โดยมุ่งเน้นศึกษาวิเคราะห์หลักกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกติการะหว่างประเทศ หลักกฎหมายต่างประเทศ และหลักกฎหมายของประเทศไทยที่เกี่ยวข้องต่างๆ โดยเฉพาะอย่างยิ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และนำหลักการของพระราชบัญญัติทั้งสองฉบับนี้มาวิเคราะห์เปรียบเทียบเพื่อหาแนวทางในการพัฒนาหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยต่อไป

ผลการวิจัย

หลักการคุ้มครองข้อมูลส่วนบุคคล เกิดขึ้นโดยผลของการที่นานาอารยะประเทศยอมรับในแนวคิดเรื่องสิทธิในความเป็นส่วนตัว อันหมายถึงสิทธิที่จะอยู่โดยลำพัง โดยปราศจากการแทรกแซงและล่วงละเมิดจากบุคคลอื่น โดยเราสามารถมองสิทธิในความเป็นส่วนตัวออกได้เป็นสองแง่มุม คือ ความเป็นส่วนตัวในแง่นามธรรม ได้แก่การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ความรู้สึกนึกคิดตลอดจนความเชื่อในทางศาสนา และ ส่วนความเป็นส่วนตัวในทางรูปธรรมคือสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวนและแทรกแซงจากบุคคลอื่น การอยู่อย่างสันโดยไม่ติดต่อสัมพันธ์กับสังคม และภายใต้แนวคิดนี้ ข้อมูลของบุคคลใดก็ตามที่สามารถเก็บรักษาความลับเกี่ยวกับตัวบุคคลนั้น ก็ย่อมมีสิทธิได้รับการคุ้มครองตามกฎหมายจากการละเมิดของบุคคลอื่น ซึ่งบุคคลอื่นนี้ย่อมหมายถึงทั้งรัฐไม่ว่าจะเป็นองค์กร หน่วยงาน หรือเจ้าหน้าที่ของรัฐ และรวมถึงเอกชนด้วย ไม่ว่าจะเป็นเพื่อนบ้าน นายจ้าง หรือแม้แต่สื่อมวลชนในทุกแขนงก็ตาม สิทธิในความเป็นส่วนตัวจึงเป็นสิทธิของคนใดคนหนึ่งในส่วนที่มีลักษณะเฉพาะตัวเพื่อป้องกันตัวเองออกจากสาธารณะ บุคคลมีสิทธิที่จะปฏิเสธข้อมูลอันเป็นความลับของตนต่อสาธารณะได้ (วรรณรัชชา ทรัพย์รดาพัดชา, 2558: 8-9)

สิทธิความเป็นส่วนตัว สามารถจำแนกออกได้เป็น 4 ด้าน ดังนี้ (บรรเจิด สิงคะเนติ และคณะ, 2554: 6-7)

1. สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (Information Privacy)

เป็นสิทธิเหนือข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่อาจโดยทางตรงหรือโดยอ้อมโดยระบุหมายเลขประจำตัวประชาชน (เช่นหมายเลขประกันสังคม) หรืออย่างน้อยหนึ่งองค์ประกอบที่เป็นเอกลักษณ์ของบุคคลนั้น (เช่น ชื่อและนามสกุล, วันเดือนปีเกิด, ข้อมูลไบโอเมตริกซ์ ลายนิ้วมือ ดีเอ็นเอ ฯลฯ เป็นต้น ซึ่งจะได้รับความคุ้มครองโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล ทั้งนี้ การคุ้มครองความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัวนั้น มีหลักการสากลที่เป็นกรอบในการคุ้มครองข้อมูลส่วนบุคคล (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ซึ่งรายละเอียดจะได้กล่าวในบทต่อไป

2. สิทธิในความเป็นส่วนตัวเกี่ยวกับเนื้อตัวร่างกาย (Bodily Privacy)

ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) เป็นการให้ความคุ้มครองในชีวิตร่างกาย

ของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใดๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม การทดลองยา เป็นต้น

3. สิทธิในความเป็นส่วนตัวเกี่ยวกับการติดต่อสื่อสาร (Privacy of Communication)

เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

4.สิทธิในความเป็นส่วนตัวเกี่ยวกับการอยู่หรือพักอาศัย (Teritorial Privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะรุกล้ำเข้าไปในอาณาเขตแห่งสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวงจรปิดและการตรวจสอบหมายเลขประจำตัวประชาชนของบุคคลเพื่อการเข้าที่พักอาศัย (ID Checks)

โดยหลักการคุ้มครองข้อมูลส่วนบุคคลได้รับการยอมรับในกติการะหว่างประเทศและกฎหมายระหว่างประเทศที่สำคัญ ดังต่อไปนี้คือ

1. หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

กำเนิดขึ้นใน ปี ค.ศ. 1980 โดยองค์การร่วมมือและพัฒนาทางเศรษฐกิจ หรือ OECD ได้จัดทำคู่มือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่เรียกว่า Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ที่มีการกำหนดหลักการสำคัญไว้ 8 ประการคือ (นครเสรีรักษ์, 2558: 14-16)

1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล โดยในการจัดเก็บข้อมูลส่วนบุคคลข้อมูลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ถูกต้องและชอบด้วยกฎหมาย โดยจะต้องให้เจ้าของข้อมูลรับทราบและยินยอมในการจัดเก็บข้อมูล

2) หลักคุณภาพของข้อมูล โดยข้อมูลส่วนบุคคลที่จัดเก็บจะต้องเป็นข้อมูลที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการใช้และต้องเป็นข้อมูลที่ถูกต้องสมบูรณ์และมีการปรับปรุงให้ถูกต้องทันสมัยตรงตามความเป็นจริงเสมอ

3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ โดยต้องกำหนดวัตถุประสงค์ในการเก็บข้อมูลก่อนที่จะจัดเก็บข้อมูลส่วนบุคคลนั้น

4) หลักข้อจำกัดในการนำไปใช้ การใช้ข้อมูลจะกระทำโดยขัดต่อวัตถุประสงค์นั้นจะกระทำมิได้ เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลตามที่กฎหมายกำหนด

5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล ต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันความเสี่ยงจากการเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยโดยไม่ได้รับอนุญาต

6) หลักการเปิดเผยข้อมูล ต้องมีการกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผยข้อมูล หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูล ซึ่งต้องไม่เป็นการกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูล

7) หลักการมีส่วนร่วมของบุคคล ต้องมีการกำหนดให้ปัจเจกชนมีสิทธิต่างๆ เช่น การได้รับการแจ้งว่าข้อมูลของตนถูกจัดเก็บ สามารถตรวจสอบข้อมูลส่วนบุคคลของตน สามารถขอให้มีการแก้ไขข้อมูลที่ไม่ถูกต้อง และปฏิเสธการจัดเก็บข้อมูลส่วนบุคคลของตนเมื่อมีเหตุสมควร

8) หลักความรับผิดชอบ กำหนดความรับผิดในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล

2. หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR)

สหภาพยุโรปได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ General Data Protection Regulation (GDPR) ซึ่งจะมีผลบังคับใช้ในวันที่ 25 พฤษภาคม 2561 โดยมาแทนที่กฎหมายเดิมหรือ EU Data Protection Directive ซึ่งมีผลบังคับใช้มาตั้งแต่ปี 2538 โดยข้อบังคับฉบับนี้ให้การคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล ทั้งยังให้การรับรองว่าข้อมูลจะได้รับการคุ้มครองอย่างเท่าเทียมกันตลอดทั้งตลาดร่วมยุโรป โดยมีขอบเขตการบังคับใช้ คือ ในมาตรา 2 ได้ให้คำจำกัดความของข้อมูลส่วนบุคคล (personal data) ว่าหมายถึงข้อมูลข่าวสาร (information) ใดๆ ที่ชี้เฉพาะตัวบุคคลหรือสามารถบ่งชี้ลักษณะเฉพาะที่เกี่ยวข้องกับตัวบุคคล ซึ่งหมายถึงบุคคลธรรมดา (natural person) ที่เป็นเจ้าของข้อมูล (data subject) การชี้เฉพาะตัวบุคคลอาจเป็นไปโดยตรงหรือโดยอ้อม การอ้างอิงถึงข้อมูลส่วนบุคคล เช่น หมายเลขประจำตัว ลักษณะสำคัญทางกาย สรีระ จิตใจ สถานะทางการเงิน สังคม วัฒนธรรม ซึ่งเป็นข้อมูลที่สามารถชี้เฉพาะตัวบุคคลได้ และในขอบเขตของการบังคับใช้ทั้งในการประมวลข้อมูลโดยวิธีการปกติ (manual) และการประมวลผลข้อมูลโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอัตโนมัติ (electronic or automatic) ดังนั้น ประชาชนทุกคนในสหภาพยุโรป หน่วยงานราชการและองค์กรธุรกิจเอกชนทุกแห่งต้องสามารถให้ความมั่นใจได้ว่าได้มีการนำกฎเกณฑ์การคุ้มครองไปปฏิบัติจริงในมาตรฐานเดียวกันทั่วทั้งสหภาพยุโรป

สำหรับการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับภาคเอกชน โดยเฉพาะในบริษัทเอกชนที่ประกอบธุรกิจการค้า ต้องยึดหลักการที่เป็นสาระสำคัญดังนี้

1. สร้างมาตรการในการรักษาคุณภาพของข้อมูล

2. กำหนดมาตรการของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย

3. สร้างข้อกำหนดในการประมวลผลข้อมูลชนิดพิเศษ เช่น ข้อมูลส่วนตัวโดยเฉพาะหรือข้อมูลอ่อนไหว (sensitive data)

4. รับรองสิทธิในการได้รับแจ้งการเก็บข้อมูลต่างๆ ของเจ้าของข้อมูล

5. รับรองสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล

6. รับรองสิทธิในการคัดค้านการประมวลผลของเจ้าของข้อมูล

7. สร้างมาตรฐานการรักษาความปลอดภัยในการประมวลผลข้อมูล

8. สร้างมาตรฐานการส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม

ต่อมาเมื่อสหภาพยุโรป ได้ตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR ก็ได้พัฒนาเพิ่มเติมหลักการเดิม EU Data Protaction Diretive ข้างต้น โดยมีสาระสำคัญดังนี้

1. กำหนดขอบเขตการบังคับใช้เชิงพื้นที่

GDPR บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ใน EU ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน นั่นคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลใน EU ไม่ว่าการประมวลผลจะทำใน EU หรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง EU และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิด

ขึ้นใน EU หากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิก EU (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนใน EU ด้วย

2. บทลงโทษ

ในกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่นกรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบ การไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำ Privacy Impact Assessment

3. การให้ความยินยอม

หลักความยินยอมได้รับการยืนยันเข้มแข็งมากขึ้น โดยระบุว่าการขอความยินยอมต้องดำเนินการในรูปแบบที่เข้าใจได้และสามารถเข้าถึงได้สะดวก (Intelligible and easily access) ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอคำยินยอม โดยการขอความยินยอมต้องมีความชัดเจน ใช้ภาษาที่ง่ายต่อการเข้าใจ นอกจากนี้การยกเลิกการให้ความยินยอมต้องดำเนินการได้ด้วยความสะดวก

ภายใต้ GDPR มีการกำหนดสิทธิของเจ้าของข้อมูลที่ชัดเจนมากขึ้นดังนี้

1. สิทธิที่จะได้รับแจ้งเมื่อเกิดความเสียหาย (Breach Notification)

ภายใต้ GDPR ถือว่าการแจ้งเป็นหน้าที่ที่ต้องปฏิบัติ เมื่อเกิดความเสียหายหรือการรั่วไหลของข้อมูล ซึ่งเกิดผลกระทบมีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ทั้งนี้การแจ้งต้องดำเนินการภายใน 72 ชั่วโมง โดยผู้ประมวลผลต้องแจ้งต่อลูกค้าและผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากเกิดความเสียหาย

2. สิทธิที่จะรู้และเข้าถึงข้อมูล (Right to Access)

เจ้าของข้อมูลมีสิทธิที่จะได้รับการแจ้งจากผู้ควบคุมข้อมูลว่า มีการประมวลผลข้อมูลหรือไม่ การประมวลผลดำเนินการที่ไหน มีวัตถุประสงค์อะไร และเมื่อร้องขอ ผู้ควบคุมข้อมูลจะต้องจัดหาสำเนาข้อมูลดังกล่าวให้เจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยไม่คิดค่าใช้จ่าย ข้อกำหนดนี้เป็นการเปลี่ยนแปลงที่สำคัญในเรื่องความโปร่งใสของข้อมูลและเป็นการยืนยันความเข้มแข็งของเจ้าของข้อมูล

3. สิทธิที่จะขอให้ลบข้อมูล (Right to be Forgotten/Right to erase)

เจ้าของข้อมูลมีสิทธิ (1) ในการแจ้งให้ลบข้อมูล ระงับการเผยแพร่ หยุดการประมวลผลโดยบุคคลที่สาม (2) มีสิทธิในการแจ้งให้ลบข้อมูลที่ไม่มีส่วนเกี่ยวข้องตามวัตถุประสงค์ในการจัดเก็บครั้งแรก และ (3) มีสิทธิในการลบข้อมูลที่เจ้าของข้อมูลได้ยกเลิกความยินยอม ทั้งนี้ ผู้ควบคุมต้องใช้ดุลพินิจในการพิจารณาเปรียบเทียบสิทธิของเจ้าของข้อมูลกับประโยชน์สาธารณะในการมีอยู่ของข้อมูลนั้น

4. สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง (Data Portability)

สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง ในรูปแบบที่สามารถใช้งานได้ตามปกติรวมทั้งรูปแบบที่อ่านได้ด้วยเครื่องมือ/อุปกรณ์ (machine-readable format)

5. สิทธิที่จะได้รับความคุ้มครองตั้งแต่ต้น (Privacy by Design/Privacy by Default)

กำหนดให้มีการวางระบบความคุ้มครอง (Protection) ตั้งแต่ในโอกาสแรกของการออกแบบระบบ มากกว่าการมาเพิ่มการดำเนินการในภายหลัง โดยกำหนดว่าต้องมีการใช้มาตรการทางเทคนิคและการบริหารที่เหมาะสม โดยยึดหลักประสิทธิภาพ เพื่อให้เป็นไปตามข้อกำหนดและเป็นการคุ้มครองสิทธิเจ้าของข้อมูล

ผู้ควบคุมข้อมูลจะเก็บและและประมวลผลข้อมูลได้เพียงเท่าที่จำเป็นเพื่อให้ภารกิจสำเร็จ (data minimization) และต้องมีการจำกัดการเข้าถึงข้อมูลโดยผู้ที่ไม่มีความเกี่ยวข้องใดๆ กับการประมวลผล

6. สิทธิที่จะได้รับการคุ้มครองโดยเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officers: DPO)

ใช้ระบบการเก็บบันทึกข้อมูลภายในองค์กร (Internal Record Keeping) แทนระบบการรายงานต่อ Data Protection Authorities (DPA) และกำหนดให้มีการแต่งตั้งเจ้าหน้าที่รับผิดชอบ (DPO) สำหรับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลขนาดใหญ่ และมีภารกิจหลักในการติดตามและประมวลผลข้อมูลเป็นประจำและเป็นระบบ (Regularly and Systematic monitoring Data Subjects)

การแต่งตั้ง DPO ต้องคำนึงถึงคุณสมบัติด้านวิชาชีพและความเชี่ยวชาญด้านกฎหมายและภาคปฏิบัติ โดยอาจแต่งตั้งเจ้าหน้าที่ภายในองค์กรหรือผู้ให้บริการภายนอก ต้องแจ้งข้อมูลการติดต่อกับทาง DPA และต้องมีทรัพยากรเหมาะสมกับการปฏิบัติภารกิจและพัฒนาความรู้ความเชี่ยวชาญของ DPO ทั้งนี้ DPO มีระบบรายงานต่อผู้บริหารระดับสูง และต้องไม่ทำหน้าที่อื่นที่อาจเป็นกรณีผลประโยชน์ทับซ้อน

3. หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ

ก่อนที่สหภาพยุโรปจะได้ประกาศใช้ GDPR นั้น ประเทศอังกฤษเองได้มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลคือ Data Protection Act 1998 ได้กำหนด หลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ คือ

หลักประการที่ 1 (The First principle) คือ ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างเป็นธรรมและถูกต้องตามกฎหมาย โดยเฉพาะอย่างยิ่งจะถูกประมวลไม่ได้ เว้นแต่เป็นไปตามเงื่อนที่กฎหมายกำหนด

หลักประการที่ 2 (The Second principle) คือ จะทำการจัดเก็บข้อมูลส่วนบุคคลไว้ได้เพียงเท่าที่ระบุไว้ในวัตถุประสงค์ และจะต้องเป็นวัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น ทั้งจะต้องไม่มีการประมวลผลที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว

ในการนี้ผู้ควบคุมดูแลข้อมูลจะต้องแจ้งให้เจ้าของข้อมูล และ Commissioner ได้รู้ถึงวัตถุประสงค์ของการจัดเก็บโดยการระบุวัตถุประสงค์ไว้ในเอกสารดังต่อไปนี้

(1) หนังสือบอกกล่าวที่ผู้ควบคุมดูแลข้อมูลแจ้งไปยังเจ้าของข้อมูล หรือ

(2) ทะเบียนการจดแจ้งข้อมูลของผู้ควบคุมดูแลข้อมูลที่ให้ไว้ต่อ Commissioner

หลักประการที่ 3 (The Third principle) คือ ข้อมูลส่วนบุคคลจะต้องเพียงพอเกี่ยวข้องและไม่มากเกินไปกว่าวัตถุประสงค์ของการประมวลผลนั้น หลักการข้อนี้อาจเรียกอีกชื่อหนึ่งได้ว่า “หลักความเพียงพอ (Adequacy Principle)” กล่าวคือ ผู้ควบคุมดูแลข้อมูล จะจัดเก็บข้อมูลส่วนบุคคลเกินกว่า ความจำเป็นตามที่ ระบุไว้ในวัตถุประสงค์ของการจัดเก็บมิได้ ดังนั้น เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องและสอดคล้องกับหลักการข้อนี้ ผู้ควบคุมดูแลข้อมูลส่วนบุคคลควรจะทบทวนแบบฟอร์มการกรอกข้อมูลเพื่อ

จัดเก็บข้อมูล เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่จะทำการจัดเก็บมีเพียงพอ เกี่ยวข้องและไม่เกินกว่าวัตถุประสงค์ที่กำหนดไว้ เช่นแบบฟอร์มการสมัครงาน แบบฟอร์มสำหรับรายละเอียดของลูกค้า

หลักประการที่ 4 (The Fourth principle) คือการจัดเก็บข้อมูลส่วนบุคคลจะต้องทำให้ถูกต้องเที่ยงตรงและทันสมัยอยู่เสมอ

หลักประการที่ 5 (The Fifth principle) คือ การเก็บข้อมูลส่วนบุคคลไม่ว่าเพื่อวัตถุประสงค์ใดๆ จะต้องไม่จัดเก็บไว้นานเกินกว่าความจำเป็นเพื่อวัตถุประสงค์นั้น โดย ตามหลักทั่วไปข้อมูลส่วนบุคคลควรถูกทำลายเมื่อไม่มีความต้องการข้อมูลนั้นอีก แต่ในบางกรณีอาจมี การกำหนดให้มีการเก็บข้อมูลส่วนบุคคลนั้นได้นานกว่าปกติได้ เช่นกรณีของการอาศัยอำนาจตามกฎหมายว่าด้วยการต่อต้านการก่อการร้าย (Anti-terrorism Crime and Security Act 2001) เป็นต้น

หลักประการที่ 6 (The Sixth Principle) คือ จะต้องทำการประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องกับสิทธิของเจ้าของข้อมูลตามที่กำหนดไว้ใน Data Protection Act 1998 โดยใน Schedule 1 ของ Data Protection Act 1998 วางหลักไว้ว่าหากผู้ประมวลผลข้อมูลกระทำการดังต่อไป ให้ถือว่าเป็นการกระทำที่ฝ่าฝืนหลักการคุ้มครองข้อมูลประการที่หก

(1) ละเมิดสิทธิในการเข้าถึงข้อมูลตามที่กำหนดไว้ใน Section 7

(2) ไม่ปฏิบัติตามคำร้องขอที่สมเหตุสมผลของเจ้าของข้อมูลที่ให้ยุติการประมวลผลข้อมูลตามที่กำหนดไว้ใน Section 10 หรือไม่ปฏิบัติตามคำร้องนั้นภายใน 21 วันนับแต่วันได้รับคำร้องขอ

(3) ไม่ปฏิบัติตามคำร้องขอให้ยุติการประมวลผลข้อมูล เพื่อทำการตลาดแบบตรงตามที่กำหนดไว้ใน Section 11

(4) ปฏิบัติฝ่าฝืน Section 13 โดยไม่ปฏิบัติตามคำร้องขอเกี่ยวกับการตัดสินใจโดยอาศัยการประมวลผลของเครื่องมือที่ทางานโดยอัตโนมัติหรือการไม่แจ้งให้เจ้าของข้อมูลทราบถึงการตัดสินใจตามคำร้องนั้น หรือการไม่ตอบกลับไปยังเจ้าของข้อมูลภายใน 21 วันนับแต่วันที่ได้รับคำร้องนั้น

(5) ปฏิบัติฝ่าฝืน Section 12 a (สิทธิเฉพาะกาล (Transition Rights)) โดยการไม่ปฏิบัติตามคำบอกกล่าว (Notice) ของ Commissioner ที่ชอบด้วยกฎหมาย

หลักประการที่ 7 (The Seventh Principle) คือ ต้องจัดให้มีมาตรการทางเทคนิคและการจัดการที่เหมาะสมในการป้องกันและจัดการกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือไม่ชอบด้วยกฎหมาย และเพื่อป้องกันการสูญหายหรือการทำลายหรือทำให้เสียหายต่อข้อมูลส่วนบุคคล

หลักการข้อนี้ มีรากฐานมาจาก EU Directive (95/46/EC) มีวัตถุประสงค์เพื่อให้ผู้ควบคุมดูแลข้อมูลเกิดความระมัดระวังในการประมวลผลข้อมูล และเป็นการกำหนดมาตรการเพื่อให้เจ้าของข้อมูลเกิดความมั่นใจว่าข้อมูลส่วนบุคคลของตนจะได้รับการดูแลอย่างเหมาะสม

หลักประการที่ 8 (The Eight principle) คือข้อมูลส่วนบุคคลจะต้องไม่ถูกส่งออกไปยังประเทศหรือดินแดนที่อยู่นอกเขต European Economic Area (EEA) เว้นแต่ประเทศหรือดินแดนนั้นรับรองว่ามีระดับการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลที่เพียงพอสำหรับการประมวลผลข้อมูลส่วนบุคคล

ต่อมาภายหลังจากที่สหภาพยุโรปประกาศใช้ GDPR ส่งผลให้ประเทศอังกฤษปรับตัวโดยการตรา Data Protection Act 2018 โดยยอมรับและพัฒนาหลักการเป็นไปในแนวทางเดียวกันกับ GDPR นั่นเอง (ICO, 2021)

4. หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

เดิมกฎหมายคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศสคือ รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertès หรือ The Act on Data Processing Data Files and Individual Liberties) ที่กำหนดหลักการคุ้มครองมูลส่วนบุคคลมาช่วงระยะเวลาก่อนที่สหภาพยุโรปจะได้มีการประกาศใช้ GDPR และเมื่อได้มีการประกาศใช้แล้วก็มีผลทำให้ประเทศฝรั่งเศสทำการปรับปรุงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับ GDPR โดยเมื่อวันที่ 21 มิถุนายน พ.ศ. 2561 ได้ประกาศใช้กฎหมายฉบับใหม่ (“(“Loi n°2018-493 on the protection of personal data”)

ตามกฎหมายของประเทศฝรั่งเศสนี้ ได้มีการให้ความหมายของข้อมูลส่วนบุคคล ว่าหมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลที่ทำให้สามารถระบุหรือเปิดเผยตัวบุคคลได้ ไม่ว่าโดยตรงหรือโดยอ้อมโดย เช่นข้อมูลที่มีการอ้างอิงถึงหมายเลขประจำตัวประชาชน หมายเลขประกันสังคม หรือข้อมูลที่ระบุถึงอัตลักษณ์ทางกายภาพ สรีรวิทยา หรือจิตวิทยา ฐานะเศรษฐกิจวัฒนธรรม หรือสังคมของบุคคล ชื่อและวันเดือนปีเกิด ข้อมูล biometrics ลายนิ้วมือ รวมถึง ดีเอ็นเอ ฯลฯ เป็นต้น ทำให้สามารถจำแนกประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ดังนี้คือ

ก. ข้อมูลส่วนบุคคล (Definition of personal data)

ข้อมูลส่วนบุคคลที่เปิดเผยโดยตรงหรือโดยอ้อมเชื้อชาติและเชื้อชาติความคิดเห็นทางการเมืองปรัชญาหรือศาสนาหรือสหภาพแรงงานของบุคคลหรือที่เกี่ยวข้องกับสุขภาพหรือชีวิตทางเพศของพวกเขา

ข. ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Definition of sensitive personal data)

ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่สามารถระบุได้โดยทางตรงหรือโดยทางอ้อมโดยการอ้างอิงถึงหมายเลขประจำตัวหรือปัจจัยหนึ่งหรือหลายอย่างที่เฉพาะเจาะจงเช่นชื่อหมายเลขทะเบียนหรือหมายเลขโทรศัพท์

ซึ่งในส่วนของ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive data) ได้มีการปรับปรุงเพิ่มเติมความหมายเพื่อให้สอดคล้องกับ GDPR โดยขอบเขตของข้อมูลส่วนบุคคลที่มีความอ่อนไหว ได้รับการขยายความ รวมไปถึง ข้อมูลทางพันธุกรรมข้อมูลไบโอเมตริกซ์ และข้อมูลเกี่ยวกับการกำหนดพฤติกรรมทางเพศของเจ้าของข้อมูล

เมื่อพิจารณาถึงการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วน ได้บัญญัติรับรองสิทธิของบุคคลธรรมดาที่เกี่ยวข้องกับข้อมูลที่ระบุชื่อไว้หลายประการ ได้แก่

1. สิทธิในการสอบถามหน่วยงานของรัฐหรือ องค์กรเอกชนที่จัดทำระบบข้อมูลสารสนเทศแบบอัตโนมัติว่ามีข้อมูลส่วนบุคคลของตนหรือไม่ และสิทธิในการเข้าตรวจดูข้อมูลนั้นได้ในกรณีที่มีข้อมูลข่าวสารของตนปรากฏอยู่

2. สิทธิในการได้รับการเปิดเผยข้อมูลที่เกี่ยวกับตน ทั้งนี้ ข้อมูลที่เปิดเผยนั้นจะต้องใช้ภาษาที่เข้าใจง่ายและต้องมีเนื้อความเป็นอย่างเดียวกับข้อมูลที่บันทึกไว้

3. สิทธิในการได้รับสำเนาเอกสารข้อมูลที่เกี่ยวกับตน

4. สิทธิในการขอให้ดำเนินการแก้ไขเพิ่มเติมทำให้ชัดเจนขึ้น ปรับปรุงให้ทันสมัยหรือลบทิ้งซึ่งข้อมูลที่เกี่ยวกับตนที่ไม่ถูกต้อง ไม่ครบถ้วนสมบูรณ์ คลุมเครือ ล้าสมัย หรือการเก็บรวบรวม การใช้ การเปิดเผย หรือการเก็บรักษาข้อมูลนั้นเป็นการต้องห้าม

นอกจากที่กล่าวมายังมีสิทธิอีก 7 ประการที่ได้มีการเพิ่มเติมขึ้นในภายหลัง คือ

1. สิทธิในการโต้แย้งคัดค้านการเปิดเผยข้อมูลของตนในกรณีที่มีการนำไปใช้ประโยชน์ในทางการโฆษณาหรือวัตถุประสงค์ในทางการค้า ซึ่งบุคคลอาจคัดค้านการเปิดเผยข้อมูลของเขาต่อบุคคลที่สาม ในกรณีของการกระทำการเพื่อวัตถุประสงค์ดังกล่าวตั้งแต่ในขณะที่มีการเก็บรวบรวมข้อมูล

2. สิทธิที่จะร้องขอให้ตรวจสอบการกระทำที่เป็นการละเมิดข้อมูลส่วนบุคคลของตน

3. สิทธิที่จะได้รับการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล (Breach Notification) ภายใน 72 ชั่วโมง

4. สิทธิในการเข้าถึง (Right to Access) ที่ผู้ควบคุมข้อมูล ต้องแจ้งเจ้าของข้อมูลว่าข้อมูลถูกใช้เอาไปใช้เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

5. สิทธิที่จะถูกลืม (Right to be Forgotten) ซึ่งเจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้ตามความประสงค์

6.. สิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (Data Portability)

7. สิทธิในข้อมูลของผู้เยาว์ กฎหมายฉบับใหม่ได้มีการกำหนดให้ ผู้เยาว์ที่มีอายุต่ำกว่า 15 ปี สามารถใช้สิทธิในการคุ้มครองข้อมูลได้โดยไม่ต้องแจ้งให้บิดามารดาหรือผู้ปกครองตามกฎหมายเกี่ยวกับการประมวลผลข้อมูลด้านสุขภาพของตน สำหรับการวิจัยทางการแพทย์ การศึกษาหรือการประเมินผลบางประเภท

กฎหมายฉบับนี้ได้กำหนดให้มีองค์กรรับผิดชอบ เรียกว่า คณะกรรมการข้อมูลข่าวสารและเสรีภาพแห่งชาติ (National Commission for Data Processing and Licensing หรือ Commission nationale de l'informatiqueet des litertés: CNIL) เป็น องค์กรอิสระซึ่ง ให้คำแนะนำเกี่ยวกับการวางแผนและรับรองการประมวลผลข้อมูลข่าวสารของหน่วยงานหรือองค์กรต่างๆ คณะกรรมาธิการมีอำนาจหน้าที่ ในการแนะนำให้ความรู้เกี่ยวกับบทบัญญัติกฎหมายนี้ ในสิทธิและหน้าที่ของบุคคล รวมถึงการตรวจสอบดูแลผู้ประกอบการทางธุรกิจในการดำเนินการประมวลผลข้อมูลส่วนบุคคล นอกจากนี้ คณะกรรมาธิการต้องมีการจัดทำเอกสารเกี่ยวกับการประมวลผลข้อมูลข่าวสารในกิจกรรมต่างๆ เพื่อเผยแพร่ และจัดทำรายงานประจำปีเพื่อเสนอต่อนายกรัฐมนตรีและต่อรัฐสภา

ตามหลักคุ้มครองข้อมูลส่วนบุคคล หากพบว่ามีการปฏิบัติผิดไปจากหลักการของ General Data Protection Regulation องค์กรจะต้องจ่ายค่าปรับ 4% ของผลประกอบการรายได้ทั่วโลกทั้งหมด หรือสูงถึง 20 ล้านยูโร ซึ่งบทลงโทษนี้จะบังคับใช้ทั้งหน่วยงานผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งบทบัญญัติของกฎหมายฉบับใหม่ที่ได้มีการแก้ไขเพิ่มเติม ("("Loi n°2018-493 on the protection of personal data") ก็ได้มีการบัญญัติหลักการไว้เช่นเดียวกันกล่าวคือ หากมีการละเมิดข้อมูลส่วนบุคคล ก็จะมีบทลงโทษ

โดยมีการกำหนดค่าปรับไว้ หรือเพิกถอนการรับรองหรือการให้สิทธิ ซึ่งค่าปรับนี้ถือเป็น โทษปรับในทางปกครองซึ่งตามกฎหมายนี้ CNIL สามารถกำหนดค่าปรับได้ถึง 20 ล้านยูโรหรือคิดเป็นมูลค่าสูงสุด 4% ของมูลค่าผลประกอบการรายได้ทั่วโลกก่อนหน้าหนึ่งงรอบบัญชี

หลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เจตนารมณ์อันเป็นที่มาของกฎหมายฉบับนี้ ก็ด้วยเนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

ฐานะของกฎหมายฉบับนี้จึงมีลักษณะเป็นกฎหมายกลางที่เป็นหลักทั่วไป กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคล ของเจ้าของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลบนฐานความคิด “ปกปิดเป็นหลัก เปิดเผยเป็นข้อยกเว้น”

โดยตามพระราชบัญญัติ ระบุความหมายของ ‘ข้อมูลส่วนบุคคล’ ว่าหมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

สาระสำคัญอันเป็นหลักการคุ้มครองข้อมูลส่วนบุคคล สามารถสรุปได้ดังนี้คือ

1. องค์กรทั้งภาครัฐและเอกชนที่ดำเนินการจัดเก็บข้อมูล จะต้องมีระบบ แผนงานหรือเจ้าหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลตามมาตรฐาน ไม่ว่าองค์กรนั้นจะอยู่ในประเทศไทยหรือนอกประเทศไทยก็ตาม

2. ต้องได้รับการยินยอมจากเจ้าของข้อมูล ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล โดยต้องขอความยินยอมจากเจ้าของข้อมูลอย่างชัดเจน และต้องไม่มีเงื่อนไขในการขอความยินยอมจากเจ้าของข้อมูล

3. เจ้าของข้อมูลสามารถถอนความยินยอมเมื่อไหร่ก็ได้ โดยไม่มีข้อแม้หรือเงื่อนไข เว้นแต่จะมีข้อจำกัดสิทธิทางกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูล

4. แม้จะมีการถอนความยินยอมแล้ว ผู้ที่เก็บรวบรวมข้อมูลยังคงต้องดูแลรักษาความปลอดภัยข้อมูลเหล่านั้นไว้ หากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูล องค์กรที่เก็บรวบรวมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

5. กรณีที่เป็นเด็กอายุไม่เกิน 10 ปี ต้องได้รับความยินยอมจาก “ผู้ปกครอง” กรณีบุคคลไร้ความสามารถต้องได้รับความยินยอมจาก “ผู้อนุบาล” และกรณีบุคคลเสมือนไร้ความสามารถต้องได้รับความยินยอมจาก “ผู้พิทักษ์” โดยทั้งผู้ปกครอง, ผู้อนุบาล และผู้พิทักษ์สามารถถอนความยินยอมแทนเจ้าของข้อมูลนั้นได้

6. การเก็บข้อมูลต้องเก็บเฉพาะเท่าที่จำเป็น โดยต้องแจ้งรายละเอียดการเก็บข้อมูลให้เจ้าของข้อมูลทราบก่อนหรือระหว่างการจัดเก็บข้อมูล

7. ห้ามการจัดเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง

8. ห้ามมีการจัดเก็บข้อมูลชีวภาพ ลักษณะเด่นทางกายภาพ หรือลักษณะเด่นทางพฤติกรรมที่สามารถยืนยันตัวตนบุคคลนั้นได้ ยกเว้นการเก็บข้อมูลด้านประวัติอาชญากรรม

9. เจ้าของข้อมูลมีสิทธิ์เข้าถึงและขอรับสำเนาข้อมูลของตนเองได้ รวมถึงการขอให้เปิดเผยวิธีการได้มาซึ่งข้อมูล โดยที่เจ้าของข้อมูลไม่เคยให้ความยินยอม

10. เจ้าของข้อมูลมีสิทธิ์ในการลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้ หากข้อมูลนั้นได้มาไม่ชอบด้วยกฎหมาย

11. เจ้าของข้อมูลสามารถร้องเรียนได้ ในกรณีที่การเก็บรวบรวมข้อมูลไม่เป็นไปตามที่กฎหมายนี้กำหนดไว้

12. ผู้เก็บรวบรวมข้อมูลจะต้องชำระค่าสินไหมทดแทนแก่เจ้าของข้อมูล หากจงใจหรือประมาทจนเป็นเหตุทำให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลรั่วไหล เว้นแต่จะเกิดจากเหตุสุดวิสัย หรือเป็นคำสั่งของเจ้าหน้าที่ตามกฎหมาย

13. ผู้เก็บรวบรวมข้อมูลที่ทำให้เกิดความเสียหาย เสื่อมเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือทำให้ได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาทหรือทั้งจำทั้งปรับ หากนำข้อมูลเหล่านั้นไปแสวงหาผลประโยชน์โดยมิชอบ จะต้องระวางโทษจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

14. ผู้ที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นแล้วนำไปเปิดเผยต่อผู้อื่น โดยที่ไม่ได้รับอนุญาตทางกฎหมาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

หลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

แม้ว่ารากฐานความคิดของการตรากฎหมายข้อมูลข่าวสารของราชการจะอยู่ที่ความต้องการให้ระบบราชการมีความโปร่ง ดังนั้นในเรื่องของข้อมูลข่าวสารของราชการจึงถือหลักการที่ว่า “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น” ก็ตาม แต่สำหรับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล (ที่อยู่ในความควบคุมดูแลของหน่วยงานของรัฐ) ถือว่าเป็นส่วนหนึ่งของการคุ้มครองสิทธิส่วนบุคคลอันเป็นหลักการสำคัญเรื่องหนึ่งที่มีการระบุไว้ในเหตุผลของการประกาศใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ว่าจะต้องให้ความคุ้มครอง และยังถือได้ว่าเป็นการรองรับการคุ้มครองสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัว กรณีที่จะมีการกล่าวหรือไขข่าวแพร่หลายอันเป็นการละเมิดหรือกระทบสิทธิส่วนบุคคลในครอบครัวอันเป็นสิทธิตามรัฐธรรมนูญ ดังนั้น จึงเป็นหน้าที่ของรัฐ ไม่ว่าจะเป็นองค์กร หน่วยงาน หรือเจ้าหน้าที่ของรัฐต้องรับทราบถึงหลักปฏิบัติในการคุ้มครองข้อมูลข่าวสารส่วนบุคคล เพื่อจะได้ปฏิบัติได้ถูกต้องและไม่ละเมิดความเป็นส่วนตัวของประชาชน ซึ่งพระราชบัญญัตินี้ ได้กำหนดหน้าที่และแนวปฏิบัติสำหรับหน่วยงานต่างๆ ของรัฐไว้ ดังนี้

1. หน่วยงานของรัฐต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

2. การจัดเก็บข้อมูลข่าวสารส่วนบุคคลของผู้ใด หน่วยงานของรัฐจะต้องพยายามเก็บจากเจ้าของข้อมูลโดยตรง โดยเฉพาะในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

3. ต้องตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ โดยข้อมูลข่าวสารส่วนบุคคลที่จัดเก็บไว้อาจต้องมีการนำมาใช้เพื่อประกอบการดำเนินการเรื่องใดเรื่องหนึ่ง หากข้อมูลไม่ถูกต้องอาจจะทำให้เกิดความเสียหายต่อหน่วยงานและบุคคลที่เกี่ยวข้องได้ จึงต้องตรวจสอบแก้ไขข้อมูลให้ถูกต้องอยู่เสมอด้วย

4. ต้องจัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

5. จัดให้มีการพิมพ์ในราชกิจจานุเบกษาในเรื่องที่เกี่ยวเนื่องกับข้อมูลข่าวสารส่วนบุคคล จำนวน 6 เรื่อง รวมทั้งตรวจสอบแก้ไขข้อมูลที่นำไปพิมพ์นี้ให้ถูกต้องอยู่เสมอ ดังนี้คือ

ก. ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

การกำหนดให้หน่วยงานของรัฐต้องพิมพ์ในราชกิจจานุเบกษาว่ามีการเก็บข้อมูลข่าวสารส่วนบุคคลประเภทใดบ้าง เช่น เก็บข้อมูลส่วนบุคคลของข้าราชการทุกระดับทุกคน ของลูกจ้างทุกคนทั้งลูกจ้างประจำและลูกจ้างชั่วคราว เป็นต้น

ข. ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

หน่วยงานของรัฐต้องพิมพ์ในราชกิจจานุเบกษาว่ามีการจัดเก็บข้อมูลในระบบใด เช่น แฟ้มเอกสาร หรือเก็บในระบบคอมพิวเตอร์ เป็นต้น

ค. ลักษณะการใช้ข้อมูลตามปกติ

หน่วยงานของรัฐต้องพิมพ์ในราชกิจจานุเบกษาว่าข้อมูลข่าวสารส่วนบุคคลที่จัดเก็บไว้นี้จะมีการนำไปใช้ในเรื่องใดกรณีใดบ้าง ซึ่งจะทำให้สามารถตรวจสอบในภายหลังได้ว่ามีการใช้นอกเหนือจากที่ประกาศไว้หรือไม่

ง. วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

เนื่องจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้รับรองสิทธิจากเจ้าของข้อมูลให้สามารถขอตรวจดูข้อมูลข่าวสารส่วนบุคคลของตนเองที่หน่วยงานของรัฐจัดเก็บไว้ได้ ดังนั้น การกำหนดให้พิมพ์เรื่องนี้ในราชกิจจานุเบกษา จึงช่วยให้ผู้ที่จะใช้สิทธินี้ได้รับทราบถึงวิธีการที่จะใช้สิทธิและเป็นหลักประกันว่าหน่วยงานของรัฐจะปฏิบัติต่อผู้ใช้สิทธิอย่างเท่าเทียมกัน

จ. วิธีการขอแก้ไขเปลี่ยนแปลงข้อมูล

ข้อกำหนดในข้อนี้ก็เช่นเดียวดับข้อที่ผ่านมา เนื่องจากพระราชบัญญัติรับรองสิทธิในการขอแก้ไขเปลี่ยนแปลงข้อมูลข่าวสารส่วนบุคคลของตนเองได้ การประกาศราชกิจจานุเบกษาจึงทำให้ทุกคนได้รับทราบหลักเกณฑ์หรือวิธีการที่ชัดเจนเหมือนกัน

ฉ. แหล่งที่มาของข้อมูล

เพื่อให้ทราบว่า ข้อมูลข่าวสารส่วนบุคคลที่หน่วยงานจัดเก็บมาจากแหล่งใดบ้างมีความน่าเชื่อถือเพียงใด ผู้เกี่ยวข้องจึงอาจใช้สิทธิเพื่อขอตรวจสอบและขอให้แก้ไขได้

6. กรณีหน่วยงานของรัฐจัดเก็บข้อมูลข่าวสารส่วนบุคคลโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐจะต้องถือปฏิบัติ ดังนี้

6.1 ต้องแจ้งถึงวัตถุประสงค์ที่จะนำข้อมูลไปใช้ให้เจ้าของข้อมูลทราบล่วงหน้า หรือพร้อมกับการขอข้อมูล

6.2 ต้องแจ้งให้เจ้าของข้อมูลทราบถึงลักษณะการใช้ข้อมูลตามปกติว่าจะนำไปใช้กรณีใดบ้าง

6.3 ต้องแจ้งให้เจ้าของข้อมูลทราบด้วยว่าการขอข้อมูลเป็นกรณีที่เจ้าของข้อมูลอาจให้ข้อมูลหรือไม่ให้ข้อมูลก็ได้ หรือเป็นกรณีที่กฎหมายบังคับต้องให้ข้อมูล

7. กรณีหน่วยงานของรัฐจะจัดส่งข้อมูลข่าวสารส่วนบุคคลใดบุคคลหนึ่งที่หน่วยงานของรัฐได้จัดเก็บไว้ไปยังที่ใดที่หนึ่งอันจะทำให้หรือมีโอกาสทำให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้และเป็นกรณีที่ไม่ใช้ข้อมูลตามลักษณะปกติตามที่หน่วยงานของรัฐได้เคยแจ้งให้เจ้าของข้อมูลทราบ

อภิปรายผล

เปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

จากการวิเคราะห์เปรียบเทียบกฎหมายทั้งสองฉบับ พบว่ามีความเหมือนและความแตกต่างสำคัญดังจะกล่าวต่อไปนี้คือ

ประการแรก วัตถุประสงค์ของกฎหมาย จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีวัตถุประสงค์สำคัญต้องการให้ประชาชนได้รับทราบข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐ และคุ้มครองสิทธิส่วนบุคคลในเรื่องของข้อมูลของประชาชนที่อยู่ในความครอบครองดูแลของหน่วยงานรัฐ โดยกำหนดให้เป็นหน้าที่ของหน่วยงานรัฐและเจ้าหน้าที่ของรัฐที่จะต้องปฏิบัติให้เป็นไปตามกฎหมายเพื่อรับรองและคุ้มครองสิทธิที่จะได้รู้ (Right to Know) ของประชาชน ภายใต้แนวคิดที่ว่า “เปิดเผยข้อมูลเป็นหลัก ปกปิดเป็นข้อยกเว้น” ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายที่ถูกสร้างขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ทั้งนี้เพราะประเทศไทยยังไม่มีกฎหมายที่กำหนดคุ้มครองข้อมูลส่วนบุคคลในภาพรวมทุกชนิดทุกประเภท ดังนั้นวัตถุประสงค์หลักของกฎหมายฉบับนี้คือ “ปกปิดข้อมูลเป็นหลัก เปิดเผยเป็นข้อยกเว้น”

ประการที่สอง การกำหนดนิยามของข้อมูลส่วนบุคคลตามกฎหมาย จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 4 ได้กำหนดนิยามของคำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย” ส่วน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 ได้กำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” หมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” ในประเด็นนี้เห็นว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไม่ได้ให้ความคุ้มครองไปถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรม ซึ่งหากเกิดกรณีของการที่มีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยมิชอบ โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ตัวผู้ถึงแก่กรรมหรือทายาท กรณีเช่นนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นกฎหมายกลางก็ไม่ได้คุ้มครองไปถึง

ประการที่สาม การกำหนดตัวบุคคลผู้ได้รับความคุ้มครอง จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 21 ได้

กำหนดตัวบุคคลผู้ได้รับความคุ้มครองว่า ต้องเป็นบุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทยเท่านั้น ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 กำหนดตัวบุคคลว่าหมายถึงบุคคลธรรมดา โดยพระราชบัญญัติทั้งสองฉบับไม่ได้ให้ความคุ้มครองไปถึงข้อมูลของนิติบุคคล ซึ่งสอดคล้องกับหลักการสากล โดยหากพิจารณาคำว่า ข้อมูลส่วนบุคคล (Personal Data) ที่หมายถึงข้อมูลใดๆ อันสามารถชี้เฉพาะตัวบุคคลที่เกี่ยวข้องกับตัวบุคคลซึ่งหมายถึง บุคคลธรรมดา (Natural Person) ที่เป็นเจ้าของข้อมูล (Data Subject) นั่นเอง

ประการที่สี่ การกำหนดหน้าที่ความรับผิดชอบ จะเห็นว่า ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 กำหนดหน้าที่ความรับผิดชอบของหน่วยงานรัฐ ไว้ดังนี้คือ

1. ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานรัฐสำเร็จลุล่วงตามวัตถุประสงค์เท่านั้น และต้องยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น (มาตรา 23(1))

2. การจัดเก็บข้อมูล ให้พยายามจัดเก็บจากเจ้าของข้อมูลโดยตรง (มาตรา 23(2)) และในการจัดเก็บข้อมูลจะต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลทราบล่วงหน้า หรือพร้อมกับการขอข้อมูลด้วยว่าจะนำข้อมูลนั้นมาใช้เพื่อการอันใดและลักษณะของการใช้ข้อมูลตามปกติ (มาตรา 23 วรรคสอง)

3. จัดให้มีการพิมพ์ในราชกิจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับประเภทข้อมูลที่มีการเก็บไว้ ประเภทของข้อมูลข่าวสารส่วนบุคคล ลักษณะการใช้ตามปกติ วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล แหล่งที่มาของข้อมูล (มาตรา 23(3))

4. ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ (มาตรา 23(4))

5. จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล (มาตรา 23(5))

6. ต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ (มาตรา 23 วรรคสาม)

ส่วนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ความรับผิดชอบไว้แก่ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งนับว่าเป็นผู้มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลแตกต่างกัน กฎหมายจึงกำหนดหน้าที่และความรับผิดของสองนี้ไว้แตกต่างกันด้วย โดยจะกำหนดหน้าที่และความรับผิดสำหรับผู้ควบคุมข้อมูลไว้ค่อนข้างมาก เพราะถือว่าเป็นผู้ที่รับผิดชอบโดยตรง ตัวอย่างเช่น ผู้ควบคุมข้อมูลจะมีหน้าที่ในการจัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้ เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจ รวมถึงจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา รวมถึงมีหน้าที่แจ้งเหตุกล่าวคือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า โดยจะต้องไม่เกิน 72 ชั่วโมง และหากการละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ก็จะต้องแจ้งเหตุแห่งการละเมิดพร้อมแนวทางการเยียวยาดังกล่าวให้เจ้าของข้อมูลทราบโดยไม่ชักช้า ในส่วน

ผู้ประมวลผลข้อมูล มีการกำหนดหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลเท่านั้น ไม่มีหน้าที่ในการจัดให้มีระบบตรวจสอบเพื่อดำเนินการลบข้อมูล รวมถึงมีหน้าที่ในการแจ้งให้ผู้ควบคุมข้อมูลทราบเมื่อเกิดเหตุละเมิดข้อมูล

สำหรับในประเด็นนี้ จะเห็นว่า สำหรับหน่วยงานของรัฐนั้น ถือว่าอยู่ในฐานะเทียบได้กับผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยมีกำหนดหน้าที่ไว้อย่างใกล้เคียงกัน แต่จะเห็นว่า ในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 นั้นไม่ได้มีการกำหนดหน้าที่ในการปฏิบัติต่อข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Sensitive Data) เหมือนเช่นที่มีการกำหนดไว้ใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประเด็นนี้จึงสมควรที่จะได้มีการกำหนดหน้าที่ของหน่วยงานรัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการให้สอดคล้องกันกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อไป

ประการที่ห้า การเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 24 กำหนดว่า หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

1. ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

2. เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

3. ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

4. เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

5. ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

6. ต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

7. เป็นการให้ซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

8. ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

9. กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

ในส่วนของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 27 กำหนดหลักการว่า ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เว้นแต่กรณีที่ไม่ต้องขอความยินยอมตาม มาตรา 24 หรือ มาตรา 26 ซึ่งก็ได้แก่กรณีดังนี้

1. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่

เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล ส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

โดยจะเห็นได้ว่า พระราชบัญญัติทั้งสองฉบับมีหลักการเป็นไปในทำนองเดียวกันในประเด็นนี้

ประการที่หก สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 บัญญัติให้สิทธิสำคัญแก่เจ้าของข้อมูลข่าวสารส่วนบุคคลคือ มีสิทธิขอตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตนได้ ตามมาตรา 25 โดยเมื่อบุคคลนั้นมีคำขอเป็นหนังสือหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น นอกจากนี้ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้

ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีการกำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในลักษณะที่มากและกว้างขวางกว่า โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิ

1. สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

2. สิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้

4. สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

5. สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

6. สิทธิขอให้ข้อมูลส่วนบุคคลถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด โดยในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุม

ข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้

ซึ่งสิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีการกำหนดรับรองสิทธิไว้มากมายและกว้างขวาง และสอดคล้องกับหลักการสากล เช่น สิทธิที่จะได้รับการแจ้ง (The Right to be Informed), สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (The Right of Access), สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification), สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to be Forgotten/ The Right to Erasure), สิทธิที่จะจำกัดการประมวลผล (The Right to Restrict Processing), สิทธิที่จะโอนย้ายข้อมูล (The Right to Data Portability) และสิทธิที่จะคัดค้าน (The Right to Object)

ประการสุดท้าย ประเด็นเรื่องบทกำหนดโทษ จะเห็นว่าในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540 มิได้มีบทกำหนดโทษไว้สำหรับกรณีที่หน่วยงานของรัฐ และเจ้าหน้าที่ของรัฐ ไม่ปฏิบัติให้เป็นไปตามหลักการคุ้มครองข้อมูลข่าวสารส่วนบุคคล คงมีแต่บทบัญญัติกำหนดคุ้มครองเจ้าหน้าที่ตามมาตรา 20 โดยกำหนดว่า การเปิดเผยข้อมูลข่าวสารใดแม้จะเข้าข่ายต้องมีความรับผิดตามกฎหมายใด ให้ถือว่าเจ้าหน้าที่ของรัฐไม่ต้องรับผิดหากเป็นการกระทำโดยสุจริต ใน 2 กรณีคือ การปฏิบัติที่ถูกต้องตามกฎหมายว่าด้วยการรักษาความลับ และกรณีที่ใช้ดุลพินิจเปิดเผยข้อมูลข่าวสารโดยสมควรแก่เหตุเพื่อรักษาประโยชน์ที่สำคัญกว่า ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2560 มีบทกำหนดโทษไว้อย่างรุนแรง (ระวางโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ)

สรุป

หลักการคุ้มครองข้อมูลส่วนบุคคลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีฐานะเป็นกฎหมายกลาง กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิตินั้น ได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ แต่สำหรับในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ มุ่งเน้นคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานภาครัฐ โดยกฎหมายทั้งสองฉบับมีความเหมือนและความแตกต่างกันโดยสรุปดังตารางต่อไปนี้

ตารางที่ 1 ตารางเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	**พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**
หลักการของกฎหมายเกี่ยวกับข้อมูลข่าวสารและวัตถุประสงค์ของกฎหมาย	ปกปิดเป็นหลัก เปิดเผยเป็นข้อยกเว้น (มุ่งคุ้มครองสิทธิเจ้าของข้อมูล)	เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น (เพื่อความโปร่งใสในการบริหารงานภาครัฐ)

ตารางที่ 1 ตารางเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 (ต่อ)

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	**พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**
นิยามของข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ	ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย
ผู้ได้รับความคุ้มครอง	บุคคลธรรมดา	บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทย
การกำหนดหน้าที่ความรับผิดชอบในการให้ความคุ้มครอง	ควบคุมข้อมูลส่วนบุคคล จะต้อง 1. จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลไม่ได้ให้ความยินยอม และมีการกำหนดหลักการห้ามเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ 2. จัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้ เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจ 3.จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา 4. หน้าที่แจ้งเหตุ กล่าวคือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล	หน้าที่ของหน่วยงานรัฐ (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) จะต้อง 1. จัดระบบข้อมูลข่าวสารส่วนบุคคล เท่าที่เกี่ยวข้องและจำเป็นตามวัตถุประสงค์ และต้องยกเลิกเมื่อหมดความจำเป็น 2. การจัดเก็บข้อมูลให้พยายามจัดเก็บจากเจ้าของโดยตรง 3. จัดให้มีการตรวจสอบและแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ 4. จัดระบบการรักษาความปลอดภัยให้แก่ระบบข้อมูลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายกับเจ้าของข้อมูล 5. แจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้
การเปิดเผยข้อมูลส่วนบุคคล	ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เว้นแต่กรณีที่ไม่ต้องขอความยินยอมตามมาตรา 24 หรือ มาตรา 26	หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่ มีเหตุตามมาตรา 24 (1)-(9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น

ตารางที่ 1 ตารางเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 (ต่อ)

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540
สิทธิของเจ้าของข้อมูล	มีการกำหนดรับรองสิทธิไว้มากมายและกว้างขวาง และสอดคล้องกับหลักการสากล เช่น สิทธิที่จะได้รับการแจ้ง (The Right to be Informed), สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (The Right of Access), สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification),สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to Be Forgotten/ The Right to Erasure), สิทธิที่จะจำกัดการประมวลผล (The Right to Restrict Processing), สิทธิที่จะโอนย้ายข้อมูล (The Right to Data Portability) และสิทธิที่จะคัดค้าน (The Right to Object)	สิทธิที่กำหนดให้แก่เจ้าของข้อมูลข่าวสารส่วนบุคคล คือ มีสิทธิขอตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตน และมีสิทธิขอให้แก้ไขเปลี่ยนแปลงให้ถูกต้อง
บทกำหนดโทษ	มีบทกำหนดโทษชัดเจนและรุนแรง	ไม่มีบทกำหนดโทษที่ชัดเจน

ข้อเสนอแนะ

1. ควรมีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อขยายขอบเขตนิยามของคำว่าข้อมูลส่วนบุคคลให้ครอบคลุมไปถึงสิทธิในความเป็นส่วนตัวของผู้ตายหรือผู้เสียชีวิตด้วย โดยควรให้มีการแก้ไขเพิ่มเติม มาตรา 6 ให้มีข้อความดังนี้ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม และให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” เพื่อให้นิยามของกฎหมายทั้งสองฉบับไม่มีความแตกต่างกัน

2. ประเด็นข้อมูลที่มีความอ่อนไหว ควรได้รับความคุ้มครองเป็นพิเศษที่เข้มข้นมากกว่าข้อมูลอื่นๆ แต่เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 26 (5) (จ) กำหนดยกเว้นสำหรับกิจการ “เพื่อประโยชน์สาธารณะที่สำคัญ” ให้สามารถเก็บข้อมูลและใช้ข้อมูลได้โดยไม่ต้องได้รับความยินยอมอย่างชัดแจ้ง ก็เท่ากับเป็นการเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลายยกประโยชน์สาธารณะขึ้นมาอ้างได้ว่าภารกิจของหน่วยงานของตนนั้น มีความสำคัญในลักษณะเป็นประโยชน์สาธารณะ ซึ่งก็จะมีผลทำให้ข้อมูลที่มีความอ่อนไหว ก็จะไม่ได้รับการคุ้มครองจากการสอดส่องของภาครัฐได้เลย ดังนั้นในการบังคับใช้กฎหมายฉบับนี้ จึงควรตีความคำว่า “ประโยชน์สาธารณะที่สำคัญ” บนพื้นฐานของการตระหนักถึงเจตนารมณ์ของกฎหมายและให้ความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลของประชาชนเป็นสำคัญ

นอกจากนี้ ในส่วนของข้อมูลที่มีความอ่อนไหวที่อยู่ภายใต้อำนาจของหน่วยงานราชการตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งไม่ได้มีการกำหนดมาตรฐานในการคุ้มครองไว้เป็นพิเศษ กรณีเช่นนี้ สมควรที่จะได้มีการแก้ไขเพิ่มเติมในกฎหมายโดยให้มีหลักการ ว่า

“ในการจัดระบบข้อมูลข่าวสารตามมาตรา

23 และ การเปิดเผยข้อมูลข่าวสารตามมาตรา 24 แห่งพระราชบัญญัตินี้ หากข้อมูลข่าวสารนั้นเป็นข้อมูลข่าวสารส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน ให้หน่วยงานของรัฐกระทำโดยระมัดระวังและจะให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างร้ายแรงเกินสมควรมิได้”

3. สมควรที่จะได้มีการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการทำหน้าที่คุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในภาครัฐด้วย

4. ควรแก้ไขเพิ่มเติมพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 โดย กำหนดให้มีหลักเกณฑ์รักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคลที่มีการเปิดเผยข้อมูล หรือแลกเปลี่ยนข้อมูลกัน รวมถึงการเปิดเผยและการแลกเปลี่ยนข้อมูลกันด้วยวิธีอิเล็กทรอนิกส์ระหว่างหน่วยงานของรัฐ

5. แก้ไข เพิ่มเติมอำนาจของคณะกรรมการข้อมูลข่าวสาร ให้เข้ามามีบทบาทคุ้มครองสิทธิของประชาชนในการเข้าถึงข้อมูลและเสนอความเห็นเพื่อปรับปรุงกฎหมายที่เกี่ยวข้องได้

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณคณะนิติศาสตร์ มหาวิทยาลัยมหาสารคามได้ช่วยสนับสนุนทุนวิจัยและอำนวยความสะดวกให้การวิจัยครั้งนี้ลุล่วงด้วยดี

เอกสารอ้างอิง

นคร เสรีรักษ์. (2558). *การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอสำหรับประเทศไทย*. สำนักพิมพ์ฟ้าฮ่าม.

บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม. (2554). *รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว*. สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

วรรณรัชชา ทรัพย์รดาพัดชา. (2558). *ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป: ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟส์ฮาร์เบอร์ (Safe Harbour)*.[วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์].

ICO. (2021). *Guide to the UK General Data Protection Regulation (UK GDPR)*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Johnson, J. (2021). *Cyber crime: number of breaches and records exposed 2005-2020*. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/