

ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลส่วนบุคคลด้วยวงจรชีวิตข้อมูลและ  
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562\*  
The Relationship between Data Lifecycle Management and the Personal  
Data Protection Act B.E. 2562

กิตสุรณ สังขสุวรรณ\*\*

นักวิชาการอิสระ

Kitsuron Sangsuvan

Independent Scholar

วันที่รับบทความ 12 กันยายน 2566; วันแก้ไขบทความ 16 ตุลาคม 2566; วันตอบรับบทความ 13 ธันวาคม 2566

บทคัดย่อ

วงจรชีวิตข้อมูลถือเป็นกระบวนการจัดการบริหารข้อมูลส่วนบุคคลในรูปแบบหนึ่งที่หน่วยงานหลาย ๆ แห่งได้นำมาปรับใช้ในปัจจุบัน วงจรชีวิตข้อมูลอาจช่วยให้หน่วยงานต่าง ๆ จัดการบริหารข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ แต่อย่างไรก็ตาม ปัญหาอาจมีว่าวงจรชีวิตข้อมูลมีความสัมพันธ์กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ โดยเฉพาะอย่างยิ่ง วงจรชีวิตข้อมูลสามารถนำมาปรับใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้หรือไม่ อีกทั้งวงจรชีวิตข้อมูลสามารถสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลได้หรือไม่เพียงใด การวิจัยนี้จึงมีวัตถุประสงค์ในการวิเคราะห์และมุ่งหาคำตอบในประเด็นปัญหาดังกล่าว การวิจัยนี้ยังใช้วิธีการวิจัยเชิงคุณภาพโดยเก็บรวบรวมข้อมูลจากหนังสือ บทความวิชาการ รายงาน ประกาศ และบทบัญญัติกฎหมาย การวิจัยพบว่าวงจรชีวิตข้อมูลสามารถนำมาปรับใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 วงจรชีวิตข้อมูลยังสามารถนำมาใช้ในการรักษาความปลอดภัยข้อมูลส่วนบุคคลด้วยเช่นกัน

คำสำคัญ: วงจรชีวิตข้อมูล, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, การรักษาความปลอดภัย

\* บทความวิจัยนี้เป็นส่วนหนึ่งของโครงการวิจัยเรื่อง “ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลส่วนบุคคลด้วยวงจรชีวิตข้อมูลและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562”

\*\* น.บ.; น.บ.ท.; LL.M. University of Illinois Chicago School of Law, Chicago, Illinois, USA; S.J.D. Indiana University Robert H. McKinney School of Law, Indianapolis, Indiana, USA; E-mail krit.bond@yahoo.com

### Abstract

Data lifecycle management is an approach to managing the flow of data. Recently, many organizations or institutions have relied on data lifecycle management. It can help organizations or institutions manage data effectively. However, a question may arise whether data lifecycle management can be used as a compliance guideline on the Personal Data Protection Act B.E. 2562. Another question may also arise whether data lifecycle management can create data security. The purpose of this research is to analyze and address those issues. Additionally, this research method is qualitative research. It collects all information from books, articles, reports, announcements, and statutes. This research has found that data lifecycle management can be used as a compliance guideline on the Personal Data Protection Act B.E. 2562. It can secure and protect personal data as well.

**Keywords:** Data Lifecycle Management, the Personal Data Protection Act B.E. 2562, Security

## 1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถือเป็นกฎหมายที่เกิดขึ้นใหม่ในประเทศไทย ซึ่งมีผลใช้บังคับเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 แต่การปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดยังคงถือเป็นเรื่องที่ยากลำบากสำหรับหน่วยงานต่าง ๆ<sup>1</sup> นอกจากนี้ การรั่วไหลของข้อมูลส่วนบุคคลหรือการล่องละเมิดข้อมูลส่วนบุคคลยังคงมีอยู่อย่างต่อเนื่อง<sup>2</sup> ทั้งนี้เพราะหน่วยงานต่าง ๆ มักไม่ยอมปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดไว้ หรืออาจขาดความเข้าใจในหลักเกณฑ์ต่าง ๆ ดังนั้น เครื่องมือหรือแนวทางที่จะช่วยให้หน่วยงานต่าง ๆ ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างถูกต้องจึงเป็นสิ่งที่มีความสำคัญ

วงจรชีวิตข้อมูล (Data Lifecycle) เป็นกระบวนการบริหารจัดการในรูปแบบหนึ่งที่ได้ถูกนำมาประยุกต์ใช้ในด้านบริหารจัดการข้อมูลส่วนบุคคล<sup>3</sup> องค์กรธุรกิจหรือหน่วยงานต่าง ๆ ที่มีชื่อเสียง เช่น บริษัท International Business Machines Corporations หรือ IBM ได้ใช้วงจรชีวิตข้อมูลในการบริหารจัดการข้อมูลส่วนบุคคลของตนด้วยเช่นกัน<sup>4</sup> ถึงแม้วงจรชีวิตข้อมูลจะเป็นประโยชน์ต่อการบริหารจัดการข้อมูลส่วนบุคคล แต่วงจรชีวิตข้อมูลยังคงถือเป็นเรื่องที่เกิดขึ้นใหม่สำหรับประเทศไทย ดังนั้น ประเด็นที่จำเป็นต้องศึกษาและวิจัยจึงมีอยู่ว่าวงจรชีวิตข้อมูลมีความเกี่ยวข้องหรือสัมพันธ์กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ และวงจรชีวิตข้อมูลสามารถนำมาปรับใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้หรือไม่เพียงใด รวมถึงวงจรชีวิตข้อมูลสามารถสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลได้หรือไม่เพียงใด การศึกษาและวิจัยดังกล่าวยังอาจช่วยสร้างหรือพัฒนาหลักเกณฑ์ที่สำคัญของวงจรชีวิตข้อมูล

## 2. วัตถุประสงค์ของการวิจัย

บทความนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาและพิจารณาความหมาย รูปแบบ วัตถุประสงค์ และประโยชน์ของวงจรชีวิตข้อมูล (2) ศึกษาและวิเคราะห์ว่า วงจรชีวิตข้อมูลมีความสัมพันธ์และสามารถนำมาปรับใช้กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้หรือไม่และอย่างไร (3) ศึกษาและประเมิน

<sup>1</sup> ศิริญา ดุสิตนานนท์, 'ปัญหาและข้อเสนอแนะในการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562' (2565) 25 วารสารสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ 154, 160.

<<https://ejournals.swu.ac.th/index.php/JOS/article/view/14420>> สืบค้นวันที่ 25 เมษายน 2566.

<sup>2</sup> ผู้จัดการออนไลน์, 'เปิดโปงภัยร้ายที่ซ่อนอยู่ในการละเมิดข้อมูล' (MGR ONLINE, 19 เมษายน 2566)

<<https://mgronline.com/cyberbiz/detail/9660000036411>> สืบค้นวันที่ 25 เมษายน 2566.

<sup>3</sup> Ralph M. Stair & George W. Reynolds, *Fundamentals of Information Systems* (9th edn, Cengage Learning 2018) 139.

<sup>4</sup> *ibid* 634.

ว่าวงจรชีวิตข้อมูลสามารถนำมาใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้หรือไม่และอย่างไร (4) สร้างหรือพัฒนาหลักเกณฑ์สำคัญของวงจรชีวิตข้อมูลด้วยหลักกฎหมายดังกล่าว และ (5) ศึกษาและวิเคราะห์ว่า วงจรชีวิตข้อมูลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลได้หรือไม่

### 3. วิธีการดำเนินการวิจัย

การศึกษาและวิเคราะห์ถึงความสัมพันธ์ระหว่างวงจรชีวิตข้อมูลและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือการปรับใช้วงจรชีวิตข้อมูลในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีเก็บรวบรวมข้อมูลจากหนังสือ บทความวิชาการ รายงาน ประกาศ บทบัญญัติกฎหมายทั้งในประเทศไทยและต่างประเทศ ข้อมูลทั้งหมดนี้ได้ถูกนำมาใช้ในการวิเคราะห์รูปแบบวงจรชีวิตข้อมูลและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกจากนี้ ข้อมูลดังกล่าวได้ถูกนำมาใช้ในการวิเคราะห์ถึงการรักษาความปลอดภัยข้อมูลส่วนบุคคลด้วยวงจรชีวิตข้อมูล

### 4. ผลการวิจัย

การวิจัยพบว่าวงจรชีวิตข้อมูลมีความเกี่ยวข้องหรือสัมพันธ์กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยวงจรชีวิตข้อมูลสามารถนำมาใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งหากผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้วงจรชีวิตข้อมูลเป็นแนวทางในการบริหารจัดการข้อมูลส่วนบุคคล ก็ย่อมมีความเป็นไปได้ที่ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้อย่างถูกต้องและมีประสิทธิภาพ นอกจากนี้ วงจรชีวิตข้อมูลยังอาจนำมาใช้ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วยเช่นกัน

### 5. อภิปรายผลการวิจัย

#### 5.1 วงจรชีวิตข้อมูล

##### 5.1.1 ความหมายและรูปแบบของวงจรชีวิตข้อมูล

วงจรชีวิตข้อมูล คือ กระบวนการจัดการข้อมูลผ่านวิวัฒนาการหรือรอบวงจรชีวิต โดยเริ่มต้นจากการเก็บข้อมูลจนถึงการทำลายข้อมูล<sup>5</sup> การจัดการข้อมูลด้วยวงจรชีวิตข้อมูลช่วยทำให้องค์กรธุรกิจ

<sup>5</sup> Roger S. Reid, Gareth Fraser-King, David Schwaderer, *Data Lifecycle: Managing Data for Strategic Advantage* (Wiley 2007) 13.

หรือผู้ควบคุมข้อมูลสามารถบริหารหรือดูแลข้อมูลได้อย่างเป็นระบบและมีประสิทธิภาพ<sup>6</sup> วงจรชีวิตข้อมูลยังมีความสัมพันธ์กับการคุ้มครองความเป็นส่วนตัวของข้อมูล (Data Privacy) ที่มุ่งเน้นให้ความสำคัญคุ้มครองและปฏิบัติตามกฎหมาย รวมไปถึงการปกป้องข้อมูลต่างๆ โดยวิธีการรวบรวม ประมวลผล การเปิดเผยข้อมูล การจัดเก็บ และการลบข้อมูลนั้น ๆ นอกจากนี้ วงจรชีวิตข้อมูลมีวัตถุประสงค์ที่สำคัญคือ (1) เพื่อเก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality) หรือป้องกันมิให้ข้อมูลถูกเข้าถึงโดยไม่ชอบด้วยกฎหมาย (2) เพื่อให้ข้อมูลนำมาใช้ประโยชน์ได้อย่างเหมาะสมโดยชอบด้วยกฎหมาย (Availability) และ (3) เพื่อให้ข้อมูลมีความถูกต้องและทันสมัยอยู่เสมอ (Integrity)<sup>7</sup>

สำหรับวงจรชีวิตข้อมูลอาจแบ่งออกเป็น 5 ระยะดังต่อไปนี้ (1) การเกิดขึ้น (Creation) (2) การเก็บรักษา (Storage) (3) การใช้งาน (Usage) (4) การเก็บแบบถาวร (Archival) และ (5) การทำลาย (Destruction)

### (1) การเกิดขึ้น (Creation)

การเกิดขึ้น (Creation) คือ การเก็บรวบรวมหรือการได้มาซึ่งข้อมูล<sup>8</sup> การเกิดขึ้นนี้ยังถือเป็นจุดเริ่มต้นสำคัญของวงจรชีวิตข้อมูล โดยองค์กรธุรกิจอาจเก็บรวบรวมข้อมูลผ่านการทำธุรกรรมหรือช่องทางต่าง ๆ เช่น การขายสินค้าให้ลูกค้า การติดต่อสื่อสารกับลูกค้า หรือ การให้บริการหลังการขาย อีกทั้งวิธีการเก็บรวบรวมหรือการได้มาซึ่งข้อมูลอาจมีหลากหลายรูปแบบ เช่น กรอกแบบสอบถาม (Form) ตรวจสอบ (Survey) สอบถามจากลูกค้า (Interview) หรือ การเฝ้าติดตาม (Observation)<sup>9</sup> ข้อมูลที่ได้รับจึงมักมาจากแหล่งข้อมูลดั้งเดิมหรือมาจากเจ้าของข้อมูลโดยตรง แต่อย่างไรก็ตาม ไม่ได้หมายความว่าข้อมูลทุกชนิดจะเป็นที่ต้องการหรือต้องถูกนำมาเก็บรวบรวมไว้ เพราะข้อมูลบางประเภทอาจถูกนำมาใช้เป็นประโยชน์ ในขณะที่ข้อมูลบางประเภทอาจไม่มีความเกี่ยวข้องกัน ดังนั้น ข้อมูลที่ถูกเก็บรวบรวมคือข้อมูลที่อาจถูกนำมาใช้เป็นประโยชน์ได้<sup>10</sup> โดยองค์กรธุรกิจจะเป็นผู้ประเมินว่าข้อมูลใดมีความจำเป็นที่จะต้องนำมาใช้ และข้อมูลใดไม่มีความจำเป็นที่จะต้องนำมาใช้

<sup>6</sup> Nijaz Bajgoric, *Always-On Enterprise Information Systems for Business Continuity: Technologies for Reliable and Scalable Operations* (Business Science Reference 2010) 143.

<sup>7</sup> Ruben Zeegers & Theo Wanders, *Privacy & Data Protection Essentials* (Van Haren 2019) 144.

<sup>8</sup> Tibor Koltay, *Research Data Management and Data Literacies* (Chandos Publishing 2022) 92.

<sup>9</sup> *ibid.*

<sup>10</sup> Lisa Federer, *The Medical Library Association Guide to Data Management for Librarians* (Rowman & Littlefield 2016) 92.

## (2) การเก็บรักษา (Storage)

การเก็บรักษาข้อมูลเป็นขั้นตอนที่เกิดขึ้นหลังจากการเก็บรวบรวมหรือการได้มาซึ่งข้อมูล การเก็บรักษาข้อมูลในขั้นตอนนี้เป็นการทำบันทึกและเก็บรักษาข้อมูลไว้เพื่อที่จะนำไปใช้ในอนาคต<sup>11</sup> โดยข้อมูลที่ได้มาอาจถูกแปรสภาพหรือเปลี่ยนรูปแบบ และนำมาจัดเก็บไว้ในสภาพแวดล้อมที่เหมาะสมและปลอดภัย องค์กรธุรกิจยังคงใช้มาตรการรักษาความปลอดภัยหรือจัดทำสำเนาเพื่อป้องกันการสูญหาย<sup>12</sup> นอกจากนี้ การเก็บรักษาข้อมูลอาจอยู่ในรูปของชุดข้อมูล (Dataset) หรือ ระบบฐานข้อมูล (Database) สำหรับการเก็บข้อมูลในระบบฐานข้อมูล คือ การเก็บรวบรวมข้อมูลต่าง ๆ เข้าไว้ด้วยกันอย่างเป็นระบบและข้อมูลนั้นมีความสัมพันธ์ซึ่งกันและกัน<sup>13</sup> ในขณะที่การเก็บข้อมูลในรูปของชุดข้อมูล คือ การนำข้อมูลที่มีคุณสมบัติเหมือนกันมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูล<sup>14</sup> การเก็บข้อมูลในรูปของชุดข้อมูลยังอาจอยู่ในรูปแบบของดิจิทัล เช่น คลาวด์ หรือรูปแบบของกายภาพ เช่น แฟลชไดรฟ์ แผ่นซีดี ทำสำเนาหรือบันทึกลงบนกระดาษ

## (3) การใช้งาน (Usage)

การใช้ข้อมูล คือ การนำเอาข้อมูลที่ผ่านมาผ่านกระบวนการเก็บรักษามาใช้ในกิจกรรมทางธุรกิจ หรือ ก่อให้เกิดผลลัพธ์ในทางธุรกิจ<sup>15</sup> สำหรับวิธีใช้ข้อมูลนั้นย่อมขึ้นอยู่กับประเภทของข้อมูลและวัตถุประสงค์ในการใช้ข้อมูลขององค์กรธุรกิจนั้น<sup>16</sup> แต่โดยทั่วไปนั้น ข้อมูลมักถูกใช้ในการกำหนดยุทธศาสตร์หรือทิศทางขององค์กร ตรวจสอบสินค้าหรือความต้องการของลูกค้า ประมวลผล หรือปรับปรุงสินค้าหรือการให้บริการ อีกทั้งองค์กรธุรกิจยังอาจใช้ข้อมูลในการตัดสินใจหรือประกอบกิจกรรมต่าง ๆ เช่น เบอร์โทรศัพท์ของลูกค้า ได้ถูกนำมาใช้ในการติดต่อลูกค้า การใช้ข้อมูลนี้ยังจะต้องเป็นการใช้โดยผู้ที่มีอำนาจหรือผู้ที่มิหน้าที่ ๆ จะต้องรับผิดชอบโดยเฉพาะเท่านั้น

<sup>11</sup> Evren Eryurek et al., *Data Governance The Definitive Guide: People, Processes, and Tools to Operationalize Data Trustworthiness* (O' Reilly 2021) 88.

<sup>12</sup> *ibid.*

<sup>13</sup> Oracle Cloud Infrastructure, What Is a Database?, (OCI) <<https://www.oracle.com/database/what-is-database/#:~:text=A%20database%20is%20an%20organized,electronically%20in%20a%20computer%20system>> accessed 26 April 2023.

<sup>14</sup> Tech Target Contributor, Definition: data set, (Tech Target) <<https://www.techtarget.com/whatis/definition/data-set#:~:text=A%20data%20set%20is%20a,managed%20as%20a%20whole%20entity.>> accessed 26 April 2023.

<sup>15</sup> Angelo Illumba, 'What Is Data Usage?' (WhistleOut, 27 October 2021)

<<https://www.whistleout.com/CellPhones/Guides/what-is-data-usage>> accessed 26 April 2023.

<sup>16</sup> *ibid.*

## (4) การเก็บรักษาแบบถาวร (Archival)

เมื่อวันเวลาผ่านไป ข้อมูลอาจมีความล้าหลังและไม่อาจใช้ประโยชน์ได้อีก แต่ข้อมูลเหล่านี้ยังคงมีความสำคัญและอาจถูกนำกลับมาใช้ได้ในอนาคต การเก็บรักษาข้อมูลแบบถาวรจึงมีความจำเป็นต่อองค์กรธุรกิจ โดยการเก็บข้อมูลแบบถาวร (Archival) มีความหมายคือ การเก็บรักษาข้อมูลเก่าที่ไม่อาจใช้การได้หรือข้อมูลที่ไม่ได้ถูกนำมาใช้เป็นประจำ เพื่อที่จะได้นำกลับมาใช้อีกเมื่อมีความจำเป็น หรือเพื่อรอเวลาที่จะนำมาทำลาย<sup>17</sup> ข้อแตกต่างระหว่างการเก็บข้อมูลแบบถาวรและการเก็บรักษาข้อมูล (Storage) ในขั้นตอนที่สอง คือ การเก็บข้อมูลแบบถาวรเป็นการเก็บรักษาข้อมูลเก่าที่ได้มีการใช้งานมาแล้ว ในขณะที่การเก็บรักษาข้อมูล (Storage) ในขั้นตอนที่สองเป็นการเก็บรักษาข้อมูลที่ยังใช้งานหรือปฏิบัติการได้อยู่ นอกจากนี้ การเก็บรักษาข้อมูลแบบถาวรอาจช่วยลดปริมาณข้อมูลที่มีมากจนเกินไปและลดภาระในการดูแลรักษา การเก็บรักษาข้อมูลแบบถาวรจึงช่วยให้องค์กรธุรกิจจัดการบริหารข้อมูลที่มีอยู่ได้อย่างมีประสิทธิภาพ การเก็บรักษาข้อมูลแบบถาวรยังอาจมีลักษณะเป็นการเก็บรักษาในระยะยาว การเก็บรักษาจึงควรคำนึงถึงความปลอดภัยและความสะดวกในการเข้าถึง องค์กรธุรกิจควรต้องพิจารณาว่าข้อมูลชนิดใดควรจัดเก็บรักษาแบบถาวร ระยะเวลาในการเก็บรักษา และวิธีการในการเก็บรักษา<sup>18</sup>

## (5) การทำลาย (Destruction)

การทำลายข้อมูล (Destruction) คือ กระบวนการทำลายหรือลบข้อมูลที่ได้ถูกจัดเก็บรักษาไว้ในรูปแบบต่าง ๆ ออกจากการควบคุมดูแลขององค์กรธุรกิจ<sup>19</sup> โดยข้อมูลที่ถูกทำลายมักเป็นข้อมูลที่ไม่มีความจำเป็นต่อใช้อีกต่อไปและไม่สมควรที่จะต้องเก็บรักษาไว้<sup>20</sup> เพราะการเก็บรักษาข้อมูลดังกล่าวย่อมเป็นภาระและก่อให้เกิดความเสี่ยงที่ข้อมูลนั้นจะรั่วไหลหรือถูกส่งละเมิด อีกทั้งองค์กรธุรกิจยังคงต้องรับผิดชอบข้อมูลที่อยู่ในความควบคุมของตน ดังนั้น ข้อมูลที่ถูกทำลายหรือถูกลบจึงควรเป็นข้อมูลที่ถูกเก็บรักษาแบบถาวร (Archival) และเมื่อการทำลายข้อมูลนี้ถือเป็นขั้นตอนสุดท้ายของวงจรชีวิตข้อมูล การทำลายข้อมูลในขั้นตอนนี้จึงควรเป็นการทำลายข้อมูลโดยสิ้นเชิง กล่าวคือ องค์กรธุรกิจอาจใช้วิธีการใด ๆ ที่ทำให้ข้อมูลนั้นไม่สามารถนำกลับมาใช้ประโยชน์ได้อีก บุคลากรในองค์กรธุรกิจก็ไม่สามารถเข้าถึงหรือแบ่งปันข้อมูลนั้นได้นอกจากนี้ การทำลายข้อมูลควรดำเนินการด้วยความระมัดระวังและความปลอดภัยเพื่อป้องกันมิให้ข้อมูลเกิดการรั่วไหล

<sup>17</sup> Yunfei Du & Hammad Rauf Khan, *Data Science for Librarians* (ABD-CLIO 2020) 12.

<sup>18</sup> *ibid.*

<sup>19</sup> Sheng-Lung Peng, Souvik Pal & Lianfen Huang, *Principles of Internet of Things (IOT) Ecosystem: Insight Paradigm* (Springer 2020) 394.

<sup>20</sup> *ibid.*

### 5.1.2 ประโยชน์ของวงจรชีวิตข้อมูล

วงจรชีวิตข้อมูลอาจมีประโยชน์ต่อองค์กรธุรกิจดังต่อไปนี้

(1) การปฏิบัติตามกฎหมายและการบริหารจัดการ (Compliance and Governance): วงจรชีวิตข้อมูลมักเกี่ยวข้องกับหรืออาศัยแนวทางของบทบัญญัติแห่งกฎหมายเป็นสำคัญ การจัดการบริหารข้อมูลบนพื้นฐานของวงจรชีวิตข้อมูลจึงช่วยให้องค์กรธุรกิจสามารถปฏิบัติตามกฎหมายได้อย่างถูกต้อง นอกจากนี้ วงจรชีวิตข้อมูลยังช่วยให้องค์กรธุรกิจจัดการบริหารข้อมูลได้อย่างเหมาะสม มีประสิทธิภาพ และปลอดภัย รวมถึงนำข้อมูลมาใช้เพื่อให้เกิดประโยชน์สูงสุด โดยองค์กรธุรกิจอาจนำวงจรชีวิตข้อมูลมาพัฒนาเป็นแนวทางในการจัดการบริหารข้อมูลภายในองค์กร<sup>21</sup>

(2) การปรับปรุงกระบวนการ (Process Improvement): วงจรชีวิตข้อมูลถือเป็นกระบวนการจัดการข้อมูลอย่างเป็นระบบเพื่อนำข้อมูลมาใช้ให้เกิดประสิทธิภาพสูงสุด วงจรชีวิตข้อมูลช่วยรักษาคุณภาพของข้อมูล และจัดการบริหารข้อมูลอย่างมีประสิทธิภาพ วงจรชีวิตข้อมูลยังช่วยให้ข้อมูลมีความถูกต้อง ทันสมัย สามารถเข้าถึงได้ง่าย น่าเชื่อถือ และนำมาใช้งานได้สะดวก หากองค์กรธุรกิจไม่ได้จัดการบริหารข้อมูลบนพื้นฐานของวงจรชีวิตข้อมูล มีความเป็นไปได้ที่องค์กรธุรกิจนั้นจะประสบกับปัญหาหรือเผชิญกับความเสียหาย อันเนื่องมาจากการจัดการบริหารข้อมูลที่ผิดพลาด วงจรชีวิตข้อมูลจึงอาจถูกนำมาใช้ในการพัฒนาหรือปรับปรุงกระบวนการจัดการบริหารข้อมูลให้มีประสิทธิภาพ<sup>22</sup>

(3) การรักษาความปลอดภัย (Security): ปัญหาหรือความท้าทายที่องค์กรธุรกิจมักต้องเผชิญคือการรักษาความปลอดภัยของข้อมูล วงจรชีวิตข้อมูลจึงถือเป็นกระบวนการจัดการที่สำคัญเพราะช่วยลดความเสี่ยงและปกป้องคุ้มครองข้อมูลมิให้สูญหาย ถูกทำลาย หรือถูกล่วงละเมิด โดยวงจรชีวิตข้อมูลมีการกำหนดวิธีการดำเนินการในแต่ละขั้นตอนอย่างเป็นระบบและมีการตรวจสอบอย่างถี่ถ้วน หากองค์กรธุรกิจดำเนินการตามวงจรชีวิตข้อมูลได้อย่างถูกต้อง ข้อมูลที่อยู่ในการควบคุมดูแลขององค์กรธุรกิจย่อมมีความปลอดภัย<sup>23</sup>

(4) การควบคุมค่าใช้จ่าย (Controlling Costs): วงจรชีวิตข้อมูลช่วยควบคุมหรือลดค่าใช้จ่ายให้แก่องค์กรธุรกิจ ตัวอย่างเช่น ข้อมูลที่ไม่เป็นประโยชน์ต่อธุรกิจหรือไม่อาจใช้ประโยชน์ได้อีกควรทำลายทิ้ง หากองค์กรธุรกิจเลือกที่จะเก็บรักษาข้อมูลเหล่านั้น องค์กรธุรกิจอาจต้องเสียค่าใช้จ่ายหรือใช้พื้นที่ในการเก็บ

<sup>21</sup> Adam Marget, 'Data Lifecycle Management: Stages, Goals and Organizational Benefits (UNITRENDS)' <<https://www.unitrends.com/blog/data-lifecycle-management#:~:text=DLM%20allows%20organizations%20to%20make,quick%20recovery%20during%20%20crisis.>> accessed 26 April 2023.

<sup>22</sup> ibid.

<sup>23</sup> ibid.

รักษา อีกทั้งยังต้องรับภาระและความเสี่ยงในการดูแลรับผิดชอบข้อมูลเหล่านั้น แต่หากองค์กรธุรกิจตัดสินใจทำลายข้อมูล องค์กรธุรกิจก็ไม่ต้องเสียค่าใช้จ่ายในการดูแลรักษาข้อมูลซึ่งอาจมีราคาสูงกว่าการทำลายข้อมูล<sup>24</sup>

## 5.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์เพื่อป้องกันการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงได้กำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดวิธีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ พระราชบัญญัติฉบับดังกล่าวยังกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล ความรับผิดชอบทางแพ่งของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล และโทษทางอาญาหรือโทษทางปกครองที่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับ

นอกจากนี้ มาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้ (1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด” ต่อมาคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้กำหนดประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง “มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565” โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ที่สำคัญ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้กำหนดความหมายของ “ความมั่นคงปลอดภัย” ไว้คือ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการธำรงไว้ซึ่งความลับในข้อมูลส่วนบุคคล (confidentiality) ดำเนินการให้ข้อมูลส่วนบุคคลมีความถูกต้องครบถ้วน (integrity) และดำเนินการให้ข้อมูลส่วนบุคคลอยู่ในสภาพพร้อมใช้งาน (availability)

<sup>24</sup> ibid.

### 5.3 วงจรชีวิตข้อมูลและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประเด็นที่จะต้องพิจารณาอาจมีอยู่ว่า วงจรชีวิตข้อมูลมีความสัมพันธ์กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ โดยเฉพาะอย่างยิ่ง วงจรชีวิตข้อมูลสามารถนำมาปรับใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้หรือไม่เพียงใด รวมถึงวงจรชีวิตข้อมูลสามารถสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลได้หรือไม่เพียงใด

การศึกษาวิจัยพบว่า วงจรชีวิตข้อมูลสามารถนำมาใช้เป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ข้อกำหนดต่าง ๆ ภายใต้กฎหมายดังกล่าวยังอาจถูกพัฒนาเป็นหลักเกณฑ์สำคัญของวงจรชีวิตข้อมูล โดยในแต่ละขั้นตอนของวงจรชีวิตข้อมูลจะมีความเกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งหากการบริหารจัดการในแต่ละขั้นตอนของวงจรชีวิตข้อมูลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การการบริหารจัดการดังกล่าวย่อมถือเป็นการปฏิบัติตามกฎหมายได้อย่างถูกต้อง นอกจากนี้ วงจรชีวิตข้อมูลสามารถนำมาใช้ในการสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล โดยวัตถุประสงค์ของวงจรชีวิตข้อมูลคือ (1) การเก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality) (2) การทำให้ข้อมูลอยู่ในสภาพพร้อมใช้ประโยชน์ (Availability) และ (3) การทำให้ข้อมูลมีความถูกต้องและทันสมัยอยู่เสมอ (Integrity) ดังนั้น การปฏิบัติตามขั้นตอนของวงจรชีวิตข้อมูลย่อมก่อให้เกิด “ความมั่นคงปลอดภัย” ตามความหมายของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง “มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565”

สำหรับการใช้วงจรชีวิตข้อมูลเป็นแนวทางในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และสร้าง “ความมั่นคงปลอดภัย” อาจแบ่งการพิจารณาออกได้เป็นดังนี้

#### 5.3.1 ผู้มีอำนาจดำเนินการหรือบริหารจัดการในวงจรชีวิตข้อมูล

เมื่อวงจรชีวิตข้อมูลถือเป็นวิธีการจัดการบริหารข้อมูลส่วนบุคคลภายในองค์กรหรือหน่วยงานต่าง ๆ ผู้ที่มีอำนาจในการจัดการแต่ละขั้นตอนและสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลต้องเป็นบุคคลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้เท่านั้น ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ที่มีการจัดการและสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลได้แก่ (1) ผู้ควบคุมข้อมูลส่วนบุคคล และ (2) ผู้ประมวลผลข้อมูลส่วนบุคคล โดยมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดสถานะของ “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า “บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า “บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล” เมื่อเป็นเช่นนั้น เจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น ๆ ไม่ถือเป็นผู้มีอำนาจดำเนินการและสร้างความมั่นคงปลอดภัยในวงจรชีวิตข้อมูล

### 5.3.2 การเกิดขึ้น

โดยทั่วไป ขั้นตอนการเกิดขึ้น (Creation) เกี่ยวข้องกับกระบวนการเก็บรวบรวมหรือการได้มาซึ่งข้อมูลส่วนบุคคล ขั้นตอนการเกิดขึ้นจึงมักเกี่ยวข้องกับการได้มาซึ่งข้อมูลและการได้รับความยินยอม ขั้นตอนการเกิดขึ้นยังถือเป็นจุดเริ่มต้นของ “การรักษาความมั่นคงปลอดภัย” ซึ่งรวมถึงการรักษาข้อมูลไว้เป็นความลับ (Confidentiality) การทำให้ข้อมูลถูกต้องครบถ้วน (Integrity) และการทำให้ข้อมูลอยู่ในสภาพพร้อมใช้งาน (Availability) เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดวิธีการรวบรวม หรือการได้มาซึ่งข้อมูลส่วนบุคคลไว้โดยเฉพาะ ขั้นตอนการเกิดขึ้น (Creation) ในวงจรชีวิตข้อมูลที่เป็นแนวทางปฏิบัติจำต้องถือเอาหรือเป็นไปตามบทบัญญัติอันเกี่ยวกับการเก็บรวบรวมหรือการได้มาซึ่งข้อมูลส่วนบุคคล นอกจากนี้ บทบัญญัติอันเกี่ยวกับการเก็บรวบรวมหรือการได้มาซึ่งข้อมูลส่วนบุคคลได้ถูกกำหนดไว้ในหมวด 2 การคุ้มครองข้อมูลส่วนบุคคล ส่วนที่ 1 บททั่วไป และส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล โดยองค์ประกอบสำคัญของการเก็บรวบรวมข้อมูลส่วนบุคคลตามบทบัญญัติดังกล่าวได้แก่ (1) ความยินยอม (2) การแจ้งวัตถุประสงค์ (3) การแจ้งรายละเอียด (4) การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น และ (5) การเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ดังนั้น องค์ประกอบดังกล่าวนี้จำต้องถูกกำหนดไว้ในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูลเพื่อให้การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นไปอย่างถูกต้องครบถ้วนและมีประสิทธิภาพ

#### (1) ความยินยอม

##### ก. หลักทั่วไปของความยินยอม

ความยินยอม หมายถึง การที่บุคคลหนึ่งอนุญาตหรือยอมให้บุคคลอีกคนหนึ่งกระทำการอย่างใดอย่างหนึ่ง โดยบุคคลผู้อนุญาตหรือยินยอมให้ถูกกระทำนั้นยอมรับผลหรือภัยที่จะเกิดขึ้นจากการกระทำนั้น ๆ<sup>25</sup> และเมื่อบุคคลใดให้ความยินยอมในการกระทำนั้น การกระทำที่เกิดขึ้นไม่ถือว่าเป็นการละเมิดหรือเป็นการกระทำที่ผิดกฎหมาย ไม่ว่าจะบุคคลผู้นั้นจะได้รับความเสียหายอย่างไร ความยินยอมจึงถือเป็นหลักกฎหมายสำคัญที่ทำให้การกระทำไม่เป็นความผิดในทางแพ่งหรือไม่เป็นละเมิด<sup>26</sup> ตามหลักสุภาษิตว่า “ความยินยอมไม่ทำให้เป็นละเมิด” (That to which a man consents cannot be considered an injury) ดังนั้น ผู้กระทำจึงอาจกระทำการใด ๆ ต่อผู้ถูกกระทำได้โดยไม่ถือเป็นความผิด หากผู้ถูกกระทำได้ให้ความยินยอมต่อผู้กระทำ<sup>27</sup>

<sup>25</sup> วารี นาสกุล, *ประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วย ละเมิด จัดการงานนอกสั่ง และลาภมิควรได้* (พิมพ์ครั้งที่ 11, สำนักพิมพ์มหาวิทยาลัยรามคำแหง 2540) 78.

<sup>26</sup> ไพจิตร ปุญญพันธ์, *คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ลักษณะละเมิด* (พิมพ์ครั้งที่ 8, สำนักพิมพ์นิติบรรณาการ 2541) 21.

<sup>27</sup> ตัวอย่างเช่น คำพิพากษาฎีกาที่ 3776/2547 การที่จำเลยที่ 1 นำเช็คซึ่งระบุชื่อโจทก์เป็นผู้รับเงิน และเป็นเช็คมีข้อความระหว่างเส้นขีดคร่อมว่า A/C PAYEE ONLY ไปเข้าบัญชีบริษัท ก. เป็นการกระทำตามคำสั่งของจำเลยร่วมซึ่งเป็นกรรมการผู้มี

นอกจากนี้ การให้ความยินยอมของผู้ถูกระทำถือเป็นการยอมรับในความเสียหายหรือผลของการละเมิดที่เกิดขึ้น จึงถือไม่ได้ว่าผู้ถูกระทำได้รับความเสียหายนั้น<sup>28</sup>

ความยินยอมได้ถือเป็นหลักสำคัญในการเก็บรวบรวมข้อมูลส่วนบุคคล อีกทั้งยังถูกกำหนดให้อยู่ในบททั่วไปของการคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกัน โดยมาตรา 19 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น...” บทบัญญัติดังกล่าวนี้มีความหมายชัดเจนว่า การเก็บรวบรวมหรือการได้มาซึ่งข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจเก็บรวบรวมข้อมูลส่วนบุคคลโดยที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ความยินยอมต้องกระทำขึ้นก่อนหรือในขณะที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคล ความยินยอมไม่อาจเกิดขึ้นภายหลังจากที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคล เมื่อเป็นเช่นนี้ การได้รับความยินยอมจึงควรถือเป็นหลักเกณฑ์ หรือองค์ประกอบสำคัญในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในระหว่างที่อยู่ในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล

#### ข. การขอความยินยอม

การขอความยินยอม คือ การที่ผู้กระทำแสดงเจตจำนงหรือขออนุญาตต่อผู้ถูกระทำในอันที่จะกระทำการใด ๆ ต่อผู้ถูกระทำ สำหรับวิธีการขอความยินยอมนั้นได้ถูกกำหนดไว้โดยเฉพาะในมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้งเท่านั้น ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจขอความยินยอมได้โดยปริยาย อีกทั้งการขอความยินยอมต้องเป็นการแสดงออกหรือสื่อสารด้วยลายลักษณ์อักษรในรูปแบบของหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์<sup>29</sup> แต่หากผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถใช้วิธีการดังกล่าวได้ ผู้ควบคุม

---

อำนาจกระทำการแทนโจทก์ นำเช็คพิพาทเข้าบัญชีเพื่อชำระหนี้ให้แก่บริษัท ก. เจ้าหนี้โจทก์ การกระทำของจำเลยร่วมเป็นการกระทำในขอบอำนาจของกรรมการโจทก์ มีผลผูกพันโจทก์ นอกจากนี้โจทก์และบริษัท ก. ต่างก็มีกรรมการชุดเดียวกันรวม 5 คน หากกรรมการอื่นอีก 4 คน เห็นว่าจำเลยร่วมนำเช็คพิพาทไปเข้าบัญชีบริษัท ก. เป็นการไม่ถูกต้อง ก็ย่อมสามารถใช้สิทธิในฐานะเป็นกรรมการผู้มีอำนาจของบริษัท ก. สั่งให้โอนเงินตามเช็คพิพาทคืนให้แก่โจทก์ได้อยู่แล้ว การกระทำของจำเลยที่ 1 ที่ 2 และจำเลยร่วมจึงไม่เป็นละเมิดต่อโจทก์

<sup>28</sup> ตัวอย่างเช่น คำพิพากษาฎีกาที่ 673/2510 การที่โจทก์ทำให้อำนาจฟ้องเพื่อทดลองศาลอาคมซึ่งตนเชื่อถือและอวดอ้างว่าตนอยู่คงนั้น เป็นการที่โจทก์ให้ยอมหรือสมัครใจให้จำเลยทำต่อร่างกาย เป็นการยอมรับผลเสียหายที่เกิดขึ้นแก่ตนเองตามกฎหมาย จึงถือไม่ได้ว่าโจทก์ได้รับความเสียหาย โจทก์จึงฟ้องจำเลยให้รับผิดชอบชำระค่าเสียหายแก่โจทก์ไม่ได้

<sup>29</sup> มาตรา 19 วรรค 2 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้”

ข้อมูลส่วนบุคคลก็อาจเลือกใช้วิธีการอื่น ๆ เช่น บอกกล่าวหรือขอความยินยอมด้วยวาจา การขอความยินยอมยังต้องแจ้งหรือระบุวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เนื้อหาในการขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจนเพื่อป้องกันมิให้เกิดความสับสนหรือเข้าใจผิด และยังต้องทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงและเข้าใจเนื้อหาในการขอความยินยอมได้โดยง่าย ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ของการเก็บรวบรวม<sup>30</sup> นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำให้เจ้าของข้อมูลส่วนบุคคลมีอิสระในการให้ความยินยอม อีกทั้งในขณะที่เข้าทำสัญญาหรือให้บริการใด ๆ ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจกำหนดเงื่อนไขในการให้ความยินยอมสำหรับข้อมูลส่วนบุคคลที่ไม่มีความจำเป็น หรือเกี่ยวข้องกับการเข้าทำสัญญาหรือการให้บริการนั้น ๆ<sup>31</sup>

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังที่ได้กล่าวมานี้ ควรถูกนำมาปรับใช้เป็นหลักเกณฑ์หรือแนวทางปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลจำต้องขอความยินยอมให้ถูกต้องตามที่กฎหมายกำหนดในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคลหรืออยู่ในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล แต่อย่างไรก็ตาม การเก็บรวบรวมข้อมูลส่วนบุคคลโดยที่ไม่ได้ขอความยินยอมให้ถูกต้องตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจส่งผลในทางกฎหมายต่อการเก็บรวบรวมข้อมูลส่วนบุคคล โดยมาตรา 19 วรรค 7 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้” ดังนั้นจึงอาจถือได้ว่าการขอความยินยอมที่ไม่ถูกต้องตามกฎหมายย่อมไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และส่งผลให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล

<sup>30</sup> มาตรา 19 วรรค 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้”

<sup>31</sup> มาตรา 19 วรรค 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ”

### ค. การได้รับความยินยอม

การให้ความยินยอมถือเป็นการแสดงเจตนาหรือแสดงออกด้วยวิธีการใดวิธีการหนึ่ง โดยการให้ความยินยอมอาจเป็นการกระทำโดยชัดแจ้ง เช่น บอกรับด้วยวาจาหรือทำเป็นลายลักษณ์อักษร หรือการให้ความยินยอมโดยปริยาย เช่น แสดงพฤติกรรมอันเป็นที่คาดหมายได้ว่าผู้กระทำได้ให้ความยินยอมในการกระทำนั้น แม้แต่การนิ่งก็อาจถือเป็นการให้ความยินยอมได้เช่นกัน หากเป็นการนิ่งเฉยซึ่งตามพฤติกรรมนั้นสามัญชนทั่วไปเข้าใจว่าเป็นการให้ความยินยอม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้กำหนดวิธีการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลเสมือนดังเช่นการขอความยินยอมของผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องกระทำโดยชัดแจ้ง เจ้าของข้อมูลส่วนบุคคลจึงอาจให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยชัดแจ้งหรือโดยปริยายก็ได้ แต่อย่างไรก็ตาม ข้อมูลที่มีความอ่อนไหว (Sensitive Data) มีลักษณะเป็นข้อมูลลับของบุคคล (Confidential Information) ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล” ซึ่งบทบัญญัติดังกล่าวนี้ได้วางหลักเกณฑ์ทั่วไปไว้ว่า การเก็บรวบรวมข้อมูลที่มีความอ่อนไหวจำเป็นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจรับความยินยอมโดยปริยายจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้ มาตรา 19 วรรค 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังได้กำหนดให้ “ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในการเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม...” ซึ่งจากบทบัญญัตินี้ การให้ความยินยอมต้องเป็นการกระทำด้วยอำนาจการตัดสินใจของเจ้าของข้อมูลส่วนบุคคล ที่ปราศจากการถูกกลั่นแกล้ง หลอกลวง ช่มชู้ หรือสำคัญผิด อีกทั้งความยินยอมนั้นต้องไม่ขัดต่อความสำนึกในศีลธรรมอันดี<sup>32</sup>

การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนี้ควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติที่สำคัญในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล เพราะหากผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้รับความยินยอมที่ถูกต้องจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลก็ไม่สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ ขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูลก็ไม่อาจเริ่มต้นขึ้นได้ สำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับ

<sup>32</sup> ตัวอย่างเช่น คำพิพากษาฎีกาที่ 1403/2508 “ความยินยอมอันบริสุทธิ์ของผู้เสียหายให้ผู้ใดกระทำการที่กฎหมายบัญญัติเป็นความผิด ถ้าความยินยอมนั้นไม่ขัดต่อความสำนึกในศีลธรรมอันดีและมีอยู่ในขณะกระทำการอันกฎหมายบัญญัติว่า เป็นความผิดแล้ว ความยินยอมนั้นเป็นข้อยกเว้นมิให้การกระทำเป็นความผิดได้”

ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยปราศจากการหลอกลวง ช่มชู้ หรือทำให้สำคัญผิด หากผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยมีเหตุดังกล่าว การเก็บรวบรวมข้อมูลในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูลถือเป็นการไม่ชอบด้วยกฎหมาย

### ง. ข้อยกเว้นในการได้รับความยินยอม

ในบางกรณี ผู้ควบคุมข้อมูลส่วนบุคคลสามารถดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากมีเหตุตามมาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562<sup>33</sup> นอกจากนี้ มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ได้โดยไม่ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล<sup>34</sup>

<sup>33</sup> มาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุม ข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล (5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญ น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล และ (6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

<sup>34</sup> มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม (2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กร ที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิ เรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกัน

เหตุที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 24 และ 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถนำมาใช้เป็นแนวทางปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยทันทีเมื่อมีเหตุตามที่กฎหมายกำหนด

## (2) การแจ้งวัตถุประสงค์

นอกเหนือจากการขอความยินยอมโดยชัดแจ้ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล โดยมาตรา 21 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม” และมาตรา 21 วรรค 2 บัญญัติว่า “การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่ (1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน เก็บรวบรวม ใช้ หรือเปิดเผยแล้ว (2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้”

จากบทบัญญัติดังกล่าวนี้ การแจ้งวัตถุประสงค์แก่เจ้าของข้อมูลส่วนบุคคลควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติที่สำคัญอีกประการหนึ่งในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุม

---

หรืออาชีพเวชศาสตร์ การประเมินความสามารถในการทำงานของ ลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติ ตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพ หรือผู้มีหน้าที่ รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของ ข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่อ อันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพ ของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือ ตามจริยธรรมแห่งวิชาชีพ (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับ การรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติ ตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูล ส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อ คุ้มครองสิทธิขั้นพื้นฐาน และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือ สถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มี มาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการ ประกาศ กำหนด และ (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครอง สิทธิขั้นพื้นฐานและประโยชน์ ของเจ้าของข้อมูลส่วนบุคคล”

ข้อมูลส่วนบุคคลต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล การแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจึงต้องกระทำต่อเจ้าของข้อมูลส่วนบุคคลเท่านั้น การแจ้งวัตถุประสงค์ยังต้องเกิดขึ้นก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการด้วยวิธีการใด ๆ ที่ทำให้เจ้าของข้อมูลส่วนบุคคลรับทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ทั้งนี้อาจเป็นการแจ้งด้วยวาจาหรือทำเป็นลายลักษณ์อักษร สำหรับวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องไม่เป็นวัตถุประสงค์ที่เป็นการต้องห้ามชัดแจ้งโดยกฎหมาย เป็นการพันวิสัย หรือเป็นการขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน ที่สำคัญ ถึงแม้มาตรา 21 วรรค 1 จะไม่ได้บัญญัติไว้โดยชัดแจ้งว่าเจ้าของข้อมูลส่วนบุคคลจะต้องให้ความยินยอมในวัตถุประสงค์ที่ผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งไว้ แต่เมื่อการแจ้งวัตถุประสงค์เป็นสิ่งที่จะต้องดำเนินการควบคู่ไปกับการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลถูกใช้เป็นองค์ประกอบ หรือมูลเหตุในการพิจารณาหรือตัดสินใจของเจ้าของข้อมูลส่วนบุคคลว่าจะให้ความยินยอมหรือไม่ การแจ้งวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลจึงมีความเกี่ยวข้องพันกับการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล นอกจากนี้ มาตรา 21 วรรค 2 ได้กำหนดการได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์เดิมที่ได้แจ้งไว้ได้ก็ต่อเมื่อผู้ควบคุมข้อมูลส่วนบุคคลแจ้งวัตถุประสงค์ใหม่ให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนที่จะดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย ดังนั้นจึงอาจสรุปได้ว่า การแจ้งวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลควรต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

### (3) การแจ้งรายละเอียด

มาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ (1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล (3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม (4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มิได้ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการ

ติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย (6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม มาตรา 19 วรรค 5 มาตรา 30 วรรค 1 มาตรา 31 วรรค 1 มาตรา 32 วรรค 1 มาตรา 33 วรรค 1 มาตรา 34 วรรค 1 มาตรา 36 วรรค 1 และมาตรา 73 วรรค 1

การแจ้งรายละเอียดแก่เจ้าของข้อมูลส่วนบุคคลถือเป็นแนวทางปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดตามมาตรา 23 แก่เจ้าของข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม หากเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งรายละเอียดดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบ นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งรายละเอียดที่ไม่ได้ถูกกำหนดไว้ในมาตรา 23 ให้แก่เจ้าของข้อมูลส่วนบุคคล แม้เจ้าของข้อมูลส่วนบุคคลจะเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแจ้งรายละเอียดนั้นก็ตาม

#### (4) การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น

วิธีการเก็บรวบรวมข้อมูลส่วนบุคคลมีประสิทธิภาพและปลอดภัย คือ การเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น เพราะการเก็บรวบรวมข้อมูลส่วนบุคคลที่มากเกินไปหรือเกินความจำเป็นย่อมส่งผลกระทบต่อ การดูแลรักษา และอาจก่อให้เกิดปัญหาการสูญหายหรือการรั่วไหลของข้อมูล มาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงได้บัญญัติว่า “การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

การเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นนี้ควรถือเป็นหลักเกณฑ์หรือแนวปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นจะต้องใช้ ตามวัตถุประสงค์ที่กฎหมายกำหนดหรือที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล อีกทั้งดุลพินิจในการกำหนดถึงความจำเป็นในการเก็บรวบรวมข้อมูลส่วนบุคคลควรเป็นของผู้ควบคุมข้อมูลส่วนบุคคล ไม่ใช่เจ้าของข้อมูลส่วนบุคคลเป็นผู้กำหนดแต่อย่างใด นอกจากนี้ การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นช่วยสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลด้วยเช่นกัน เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลย่อมสามารถควบคุมดูแลข้อมูลส่วนบุคคลได้อย่างทั่วถึง โดยเฉพาะอย่างยิ่ง ผู้ควบคุมข้อมูลส่วนบุคคลยังสามารถ (1) เก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality) (2) ทำให้ข้อมูลอยู่ในสภาพพร้อมใช้ประโยชน์ (Availability) และ (3) ทำให้ข้อมูลมีความถูกต้องและทันสมัย (Integrity) ได้อย่างมีประสิทธิภาพ

#### (5) การเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคล

มาตรา 25 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง” แต่อย่างไรก็ตาม มาตรา 25 ตอนท้ายได้กำหนดข้อยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้มาจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ในกรณีที่

“(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26” นอกจากนี้ มาตรา 25 วรรค 2 ยังได้บัญญัติว่า “ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้ (1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว (2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าว ไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้ บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่ หรือจากการประกอบอาชีพหรือวิชาชีพ และต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด”

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง การเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคลจึงควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล แต่อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้มาจากเจ้าของข้อมูลส่วนบุคคลโดยตรงได้ หากมีเหตุตามที่กฎหมายกำหนด นอกจากนี้ การเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคลก่อให้เกิดความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล เพราะการเก็บข้อมูลส่วนบุคคลในลักษณะดังกล่าวช่วยสร้างความถูกต้องในเนื้อหาสาระของตัวข้อมูล (Integrity)

### 5.3.3 การเก็บรักษา (Storage)

การเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูล คือ การบันทึกและสงวนรักษาข้อมูล เพื่อที่จะนำไปใช้ในอนาคต การเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูลยังมีความเกี่ยวข้องกับ การรักษาความปลอดภัยในข้อมูลส่วนบุคคล<sup>35</sup> โดยการเก็บรักษาข้อมูลส่วนบุคคล (Storage) มักมีความเกี่ยวพันกับการทำให้ข้อมูลอยู่ในสภาพพร้อมใช้งาน (Availability) และการทำให้ข้อมูลมีความถูกต้องครบถ้วน (Integrity) อีกทั้งการเก็บรักษาข้อมูลส่วนบุคคลอาจช่วยป้องกันมิให้ข้อมูลส่วนบุคคลสูญหายหรือ

<sup>35</sup> Alexander Thomasian, *Storage Systems: Organization, Performance, Coding, Reliability and Their Data Processing* (Morgan Kaufmann 2021) 177.

ถูกทำลายโดยสิ้นเชิง นอกจากนี้ การเก็บรักษาข้อมูลส่วนบุคคลยังสามารถดำเนินการได้หลากหลายรูปแบบ ซึ่งก็แล้วแต่ประเภทของธุรกิจ ประเภทของข้อมูล และแนวนโยบายขององค์กรธุรกิจนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจึงอาจมีวิธีการเก็บรักษาข้อมูลส่วนบุคคลที่มีความแตกต่างกันออกไป

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้มีบทบัญญัติอันเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคลไว้โดยตรงก็ตาม แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติที่สามารถนำมาพิจารณาหรือปรับใช้ได้กับการเก็บรักษาข้อมูลส่วนบุคคล ดังนั้น บทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถนำมาใช้เป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูลได้ดังต่อไปนี้

### (1) การจัดทำสำเนา

การทำสำเนา คือ การจัดทำเอกสารให้เหมือนกับต้นฉบับ โดยอาจจัดทำจากต้นฉบับ สำเนาฉบับ หรือจากสำเนาอีกชั้นหนึ่ง การทำสำเนายังมีความหมายรวมถึง การทำสำเนาข้อมูลที่ถูกจัดเก็บไว้ในสื่อต่าง ๆ ให้มีขึ้นหลายชุดเพื่อให้เกิดความสะดวกในการจัดเก็บรักษา การทำสำเนาได้ถูกกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมาตรา 30 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน ซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคล ดังกล่าวที่ตนไม่ได้ให้ความยินยอม” จากบทบัญญัตินี้ กฎหมายไม่ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำสำเนาข้อมูลส่วนบุคคลและมอบสำเนาดังกล่าวให้แก่เจ้าของข้อมูลส่วนบุคคลเสมอ กฎหมายเพียงกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเท่านั้น เมื่อเป็นเช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องทำสำเนาข้อมูลส่วนบุคคลและมอบสำเนาดังกล่าวให้แก่เจ้าของข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ

การทำสำเนาข้อมูลส่วนบุคคลควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติในกระบวนการเก็บรักษา (Storage) ของวงจรชีวิตข้อมูล สำหรับแนวทางการทำสำเนาข้อมูลส่วนบุคคลตามมาตรา 30 วรรค 1 อาจแบ่งออกเป็น 2 กรณีคือ (1) ผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการทำสำเนาข้อมูลส่วนบุคคลไว้โดยปกติทั่วไปหรือตามแนวทางการเก็บรักษาข้อมูล และเจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนจากผู้ควบคุมข้อมูลส่วนบุคคล และ (2) ผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้ดำเนินการทำสำเนาข้อมูลส่วนบุคคลไว้ แต่เมื่อเจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิขอรับสำเนาข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจำต้องทำสำเนาข้อมูลส่วนบุคคลและส่งมอบสำเนาดังกล่าวให้แก่เจ้าของข้อมูลส่วนบุคคล การทำสำเนาข้อมูลส่วนบุคคลในกรณีดังกล่าวนี้จึงถือเป็นส่วนหนึ่งในการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นผลจากการที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิขอรับสำเนา นอกจากนี้ การทำสำเนาข้อมูลส่วนบุคคลยังช่วยก่อให้เกิดความมั่นคงปลอดภัยในข้อมูล

ส่วนบุคคล โดยเฉพาะอย่างยิ่ง การทำสำเนาข้อมูลส่วนบุคคลช่วยให้ข้อมูลส่วนบุคคลอยู่ในสภาพพร้อมนำมาใช้งาน (Availability) ทั้งนี้เพราะการทำสำเนาช่วยป้องกันมิให้ข้อมูลสูญสิ้นไปและไม่สามารถนำกลับมาใช้งานได้ อีก หรือช่วยแก้ไขหรือเยียวยาความเสียหายที่เกิดจากการที่ข้อมูลได้สูญหายหรือถูกทำลาย โดยนำสำเนาข้อมูลกลับมาใช้งานได้ตามปกติ

### (2) การทำบันทึกรายการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้มีการทำบันทึกข้อมูลส่วนบุคคล โดยมาตรา 39 วรรค 1 บัญญัติว่า “ให้ผู้ควบคุมข้อมูลส่วนบุคคลทำบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล แต่ละประเภท (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม (7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และ มาตรา 36 วรรคหนึ่ง และ (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)” จากบทบัญญัติดังกล่าวนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการทำบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบ และเตรียมความพร้อมเพื่อการใช้งาน

การทำบันทึกข้อมูลส่วนบุคคลถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติในกระบวนการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ของวงจรชีวิตข้อมูล<sup>36</sup> โดยข้อมูลส่วนบุคคลอาจถูกเก็บบันทึกไว้ในรูปแบบต่าง ๆ เช่น บันทึกลงในกระดาษ หรือ บันทึกลงในระบบอิเล็กทรอนิกส์<sup>37</sup> การทำบันทึกข้อมูลส่วนบุคคลในวงจรชีวิตข้อมูล ช่วยสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล โดยการทำบันทึกข้อมูลส่วนบุคคลอาจช่วยป้องกันไม่ให้ข้อมูลส่วนบุคคลสูญหาย และอาจถูกนำมาใช้เป็นแหล่งสืบค้นในภายหลังหรือเป็นพยานหลักฐานที่ไม่เป็นทางการ การทำบันทึกยังช่วยก่อให้เกิดความโปร่งใสในการเก็บรักษาข้อมูลส่วนบุคคลและทำให้ข้อมูลส่วนบุคคลมีความถูกต้องครบถ้วน (Integrity)

### (3) การเก็บเป็นความลับ

สาระสำคัญของการการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูล คือ การเก็บหรือ สงวนรักษาข้อมูลไว้เป็นความลับ (Confidentiality) ซึ่งหมายความว่า ข้อมูลส่วนบุคคลจะต้องมีความปลอดภัยและไม่ถูกนำไปใช้โดยผู้ที่ไม่ได้อำนาจ ผู้ควบคุมข้อมูลส่วนบุคคลจึงมีหน้าที่ ๆ สำคัญคือ

<sup>36</sup> David M. Bliesner, *Laboratory Control System Operations in A GMP Environment* (Wiley 2020) 213.

<sup>37</sup> *ibid.*

การเก็บข้อมูลส่วนบุคคลเป็นความลับหรือการไม่เปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่น นอกจากนี้ มาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคล...เปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26” ซึ่งจากบทบัญญัติดังกล่าวนี้ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลด้วยวิธีการใด ๆ แต่อย่างไรก็ตาม กฎหมายกำหนดข้อยกเว้นไว้ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นได้ หากได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยที่ได้รับยกเว้น ไม่จำเป็นต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 ดังนั้น การเก็บหรือสงวนรักษาข้อมูลไว้เป็นความลับ (Confidentiality) ควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูล เพราะการกระทำดังกล่าวสามารถสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล

#### 5.3.4 การใช้ข้อมูลส่วนบุคคล (Usage)

การใช้ข้อมูลส่วนบุคคล (Usage) คือ การที่ผู้ควบคุมข้อมูลส่วนบุคคลนำเอาข้อมูลส่วนบุคคลที่ผ่านกระบวนการเก็บรักษามาใช้ตามวัตถุประสงค์และให้เกิดประโยชน์แก่องค์กรหรือหน่วยงานของตน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีบทบัญญัติอันเกี่ยวกับการใช้ข้อมูลส่วนบุคคลไว้ โดยเฉพาะ โดยมาตรา 27 วรรค 1 ได้บัญญัติว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล...” ซึ่งจากบทบัญญัติดังกล่าวนี้ กฎหมายไม่ได้กำหนดวิธีการใช้ข้อมูลส่วนบุคคลไว้แต่อย่างใด ผู้ควบคุมข้อมูลส่วนบุคคลจึงสามารถใช้ข้อมูลส่วนบุคคลได้ในรูปแบบต่าง ๆ เพื่อให้กิจการบรรลุวัตถุประสงค์หรือเพื่อให้เกิดประโยชน์แก่องค์กรหรือหน่วยงานของตน แต่อย่างไรก็ตาม กฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล การใช้ข้อมูลส่วนบุคคลยังจะต้องไม่เป็นการใช้ที่ฝ่าฝืนบทบัญญัติแห่งกฎหมาย ดังนั้น การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการใช้ข้อมูลส่วนบุคคล (Usage) ในวงจรชีวิตข้อมูล

##### (1) การได้รับความยินยอม

การได้รับความยินยอมในการใช้ข้อมูลส่วนบุคคลตามมาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรมีความหมายและวิธีการเดียวกันกับการได้รับความยินยอมตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้เพราะมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติถึงหลักเกณฑ์ทั่วไปของการได้มาซึ่งความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล ความยินยอมตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงควรเป็นพื้นฐานและมีความสัมพันธ์กับความยินยอมในการใช้ข้อมูลส่วนบุคคล

ตามมาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนั้น การได้มาซึ่งความยินยอมตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงควรปรับใช้ได้กับความยินยอมในการใช้ข้อมูลส่วนบุคคลตามมาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

### (2) ข้อยกเว้นในการได้รับความยินยอม

มาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดข้อยกเว้นสำหรับการได้รับความยินยอมในการใช้ข้อมูลส่วนบุคคลไว้ในตอนท้ายของบทบัญญัติดังกล่าว โดยตอนท้ายของมาตรา 27 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “...เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26” ซึ่งจากข้อความดังกล่าวนี้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากข้อมูลส่วนบุคคลนั้นเป็นข้อมูลส่วนบุคคลที่สามารถเก็บรวบรวมได้โดยไม่ต้องได้รับความยินยอมตามมาตรา 24 หรือมาตรา 26

### (3) การใช้ตามวัตถุประสงค์

การใช้ข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นการใช้ตามวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล การใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ยังช่วยสร้างความมั่นคงปลอดภัยและความถูกต้องครบถ้วน แม้มาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้บัญญัติถึงวัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคลไว้ก็ตาม แต่มาตรา 21 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล และการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ดังกล่าวนี้ยังควรถือเป็นแนวทางปฏิบัติสำหรับการใช้ข้อมูลส่วนบุคคล (Usage) ในวงจรชีวิตข้อมูล

#### 5.3.5 การเก็บรักษาข้อมูลแบบถาวร (Archival)

การเก็บข้อมูลแบบถาวร (Archival) คือ การนำข้อมูลเก่าที่ไม่ใช้งานมาเก็บรักษาไว้ เพื่อที่จะได้นำกลับมาใช้อีกเมื่อมีความจำเป็น หรือเพื่อรอเวลาที่จะนำมาทำลาย แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้บัญญัติถึงวิธีการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ไว้ แต่หากพิจารณาบทบัญญัติในมาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกอบกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565” ก็อาจพบว่าการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) สามารถรักษาความมั่นคงปลอดภัย เพราะการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) อาจช่วยป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือ แก้ไขข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมถึงช่วยเก็บรักษา

ข้อมูลส่วนบุคคลไว้เป็นความลับ (Confidentiality) ทำให้ข้อมูลส่วนบุคคลถูกต้องครบถ้วน (Integrity) และทำให้ข้อมูลส่วนบุคคลอยู่ในสภาพพร้อมใช้งาน (Availability) เมื่อเป็นเช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลก็ควรเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ในวงจรชีวิตข้อมูล

นอกจากนี้ การเก็บรักษาข้อมูลส่วนบุคคลแบบถาวรมีความเกี่ยวข้องกับการทำให้ข้อมูลส่วนบุคคลมีความถูกต้องครบถ้วนและทันสมัย (Integrity) ซึ่งในกรณีดังกล่าวนี้ มาตรา 35 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด” ซึ่งบทบัญญัติดังกล่าวนี้ควรถูกนำมาปรับใช้กับการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวรด้วยเช่นกัน โดยในระหว่างการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร ผู้ควบคุมข้อมูลส่วนบุคคลจำต้องปรับปรุงหรือทำให้ข้อมูลส่วนบุคคลมีความทันสมัย ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ดังนั้น การเก็บรักษาข้อมูลส่วนบุคคลแบบถาวรจึงควรมีความหมายรวมถึง การปรับปรุงหรือทำให้ข้อมูลส่วนบุคคลมีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด อีกทั้งการปรับปรุงหรือการดำเนินการดังกล่าวนี้ยังควรถือเป็น หลักเกณฑ์หรือแนวทางปฏิบัติ สำหรับการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ในวงจรชีวิตข้อมูล

#### 5.2.6 การทำลายข้อมูล (Destruction)

การทำลายข้อมูล (Destruction) คือ การกระทำด้วยประการใด ๆ ที่ทำให้ข้อมูลส่วนบุคคลที่ถูกจัดเก็บรักษาหรืออยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถนำกลับมาใช้งานได้อีก<sup>38</sup> การทำลายข้อมูลยังอาจถือเป็นมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลด้วยเช่นกัน<sup>39</sup> เพราะเมื่อข้อมูลส่วนบุคคลถูกทำลายย่อมไม่สามารถนำกลับมาใช้ประโยชน์หรือไม่ปรากฏอีกต่อไป บุคคลภายนอกก็ย่อมไม่สามารถใช้ เข้าถึง ล่วงละเมิด หรือนำข้อมูลส่วนบุคคลนั้นเปิดเผยต่อบุคคลภายนอกได้อีก นอกจากนี้ การทำลายข้อมูลยังอาจถือเป็นการสร้างความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง การทำให้ข้อมูลส่วนบุคคลถูกเก็บรักษาไว้เป็นความลับ (Confidentiality)

สำหรับการทำลายข้อมูลส่วนบุคคลนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดการทำลายข้อมูลส่วนบุคคลไว้ออกเป็น 3 กรณีคือ

<sup>38</sup> Joanna Lyn Grama, *Legal and Privacy Issues in Information Security* (3rd edn, Jones & Bartlett Learning 2022) 374.

<sup>39</sup> Robert F. Smallwood, *Information Governance for Healthcare Professionals: A Practical Approach* (CRC Press 2018) 126.

(1) การทำลายข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคลร้องขอ

การทำลายข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคลร้องขอ คือการที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนตามที่กฎหมายกำหนดร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลของตน ทั้งนี้ มาตรา 33 วรรค 1 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้ (1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป (3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2) และ (4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้”

จากบทบัญญัติดังกล่าวนี้ เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลายข้อมูลส่วนบุคคลของตนได้ตามเหตุที่กฎหมายบัญญัติไว้ และการทำลายข้อมูลส่วนบุคคลตามมาตรา 33 วรรค 1 นี้ควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการทำลายข้อมูลส่วนบุคคล (Destruction) ในวงจรชีวิตข้อมูล

(2) การทำลายข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง

การทำลายข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง คือการที่ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลตามหน้าที่ของตน โดยที่เจ้าของข้อมูลส่วนบุคคลมิได้ร้องขอ ทั้งนี้ มาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้... (3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม...” จากบทบัญญัติดังกล่าวนี้ ผู้ควบคุมข้อมูลส่วนบุคคลสามารถลบหรือทำลายข้อมูลส่วนบุคคลด้วยตนเองโดยที่ไม่จำเป็นต้องรอให้เจ้าของข้อมูลส่วนบุคคลร้องขอ หากข้อมูลส่วนบุคคลนั้นพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น แต่อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถลบหรือทำลายข้อมูลส่วนบุคคลได้โดยทันที ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีระบบการตรวจสอบที่เหมาะสมเสียก่อนที่จะดำเนินการ เมื่อเป็นเช่นนี้ การทำลาย

ข้อมูลส่วนบุคคลตามมาตรา 37 (3) นี้ควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการทำลายข้อมูลส่วนบุคคล (Destruction) ในวงจรชีวิตข้อมูล

### (3) ข้อยกเว้นการทำลายข้อมูลส่วนบุคคล

มาตรา 33 และ 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดข้อยกเว้นในการทำลายข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องลบหรือทำลายข้อมูลส่วนบุคคลในกรณีที่ (1) การเก็บรักษามีไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น (2) การเก็บรักษามีไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26 (5) (ก) หรือ (ข) และ (3) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ซึ่งจากบทบัญญัติดังกล่าวนี้ ข้อยกเว้นในการทำลายข้อมูลส่วนบุคคลตามที่บัญญัติไว้ในมาตรา 33 และ 37 ควรถือเป็นหลักเกณฑ์หรือแนวทางปฏิบัติสำหรับการทำลายข้อมูลส่วนบุคคล (Destruction) ในวงจรชีวิตข้อมูล

## 6. บทสรุปและข้อเสนอแนะ

วงจรชีวิตข้อมูลมีความสัมพันธ์และสามารถนำมาปรับใช้ควบคู่กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยวงจรชีวิตข้อมูลสามารถนำมาใช้เป็นแนวทางปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อีกทั้งข้อกำหนดต่าง ๆ ในกฎหมายยังอาจสร้างหรือพัฒนาเป็นหลักเกณฑ์สำคัญของวงจรชีวิตข้อมูล นอกจากนี้ วงจรชีวิตข้อมูลยังก่อให้เกิดความมั่นคงปลอดภัยในข้อมูลส่วนบุคคลด้วยเช่นกัน ในเบื้องต้น ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล คือ ผู้ที่มีอำนาจบริหารจัดการในแต่ละขั้นตอนของวงจรชีวิตข้อมูลและปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูลนั้น ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล การแจ้งวัตถุประสงค์ การแจ้งรายละเอียด การเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น และการเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลส่วนบุคคลถือเป็นองค์ประกอบสำคัญของการเก็บรวบรวมข้อมูลส่วนบุคคลตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยองค์ประกอบดังกล่าวนี้ควรถือเป็นแนวทางปฏิบัติในขั้นตอนการเกิดขึ้น (Creation) ของวงจรชีวิตข้อมูล สำหรับการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมส่วนบุคคลดำเนินการทำสำเนาข้อมูลส่วนบุคคล ทำบันทึกการรายการ และเก็บข้อมูลส่วนบุคคลเป็นความลับ ดังนั้นการทำสำเนาข้อมูลส่วนบุคคล การทำบันทึกการรายการ และการเก็บข้อมูลส่วนบุคคลเป็นความลับจึงควรถือเป็นแนวทางปฏิบัติในกระบวนการเก็บรักษาข้อมูลส่วนบุคคล (Storage) ของวงจรชีวิตข้อมูล นอกจากนี้ การเก็บรักษาข้อมูลส่วนบุคคล (Storage) ในวงจรชีวิตข้อมูลยังมีความเกี่ยวข้องกับการทำให้ข้อมูลอยู่ในสภาพพร้อมใช้งาน (Availability) และการทำให้ข้อมูลมีความถูกต้องครบถ้วน (Integrity)

สำหรับการใช้ข้อมูลส่วนบุคคล (Usage) ในวงจรกิจชีวิตข้อมูล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมส่วนบุคคลดำเนินการขอความยินยอมและใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล เมื่อเป็นเช่นนี้ การขอความยินยอมและการใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ควรถือเป็นแนวทางปฏิบัติในการใช้ข้อมูลส่วนบุคคล (Usage) ในวงจรกิจชีวิตข้อมูล สำหรับการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ในวงจรกิจชีวิตข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องมีมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล “เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565” ซึ่งการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ก็ควรถือเป็นมาตรการรักษาความมั่นคงปลอดภัยในข้อมูลส่วนบุคคล นอกจากนี้ การเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ควรมีความหมายรวมถึง การปรับปรุงหรือทำให้ข้อมูลส่วนบุคคลมีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด การปรับปรุงหรือดำเนินการข้อมูลส่วนบุคคลในลักษณะดังกล่าวจึงควรถือเป็นแนวทางปฏิบัติในการเก็บรักษาข้อมูลส่วนบุคคลแบบถาวร (Archival) ของวงจรกิจชีวิตข้อมูล อีกทั้งยังถือเป็นการทำให้ข้อมูลส่วนบุคคลมีความถูกต้องครบถ้วนและทันสมัย (Integrity) สำหรับการทำลายข้อมูลส่วนบุคคล (Destruction) ในวงจรกิจชีวิตข้อมูล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้มีการทำลายข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคลร้องขอหรือทำลายข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง การทำลายข้อมูลส่วนบุคคลดังกล่าวจึงควรนำมาปรับใช้เป็นแนวทางปฏิบัติในการทำลายข้อมูลส่วนบุคคล (Destruction) ในวงจรกิจชีวิตข้อมูล อีกทั้งการทำลายข้อมูลส่วนบุคคลยังช่วยทำให้ข้อมูลส่วนบุคคลถูกเก็บรักษาไว้เป็นความลับ (Confidentiality)

แม้การวิจัยพบว่าวงจรกิจชีวิตข้อมูลสามารถถูกนำมาใช้เป็นเครื่องมือหรือแนวทางในการปฏิบัติ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่การศึกษาและวิจัยในความสัมพันธ์ระหว่างวงจรกิจชีวิตข้อมูลและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเด็นอื่น ๆ ควรดำเนินการต่อไป เช่น การศึกษาและวิจัยถึงความเป็นไปได้หรือความจำเป็นในการแก้ไขกฎหมายอันเกี่ยวกับข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับการบริหารจัดการด้วยวงจรกิจชีวิตข้อมูล หรือการนำเอาวงจรกิจชีวิตข้อมูลมาใช้เป็นมาตรการรักษาความปลอดภัยในข้อมูลส่วนบุคคลในรูปแบบใหม่ นอกจากนี้ การศึกษาและวิจัยในวงจรกิจชีวิตข้อมูลไม่ควรจำกัดหรือเชื่อมโยงกับกฎหมายแต่เพียงอย่างเดียวเท่านั้น เพราะวงจรกิจชีวิตข้อมูลถือเป็นวิธีบริหารจัดการที่มีประโยชน์ และควรนำมาศึกษาเพิ่มเติมหรือประยุกต์ใช้ในศาสตร์อื่น ๆ โดยเฉพาะอย่างยิ่ง วงจรกิจชีวิตข้อมูลควรถูกนำมาศึกษาและวิจัยในศาสตร์ด้านบริหารธุรกิจหรือเศรษฐศาสตร์