

สารบัญ

บทที่ 1 กรอบแนวคิด ทฤษฎี ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	1
1.1 ความหมายทั่วไปของความเป็นอยู่ส่วนตัว	2
1.2 ความเป็นอยู่ส่วนตัวในแง่ของสิทธิ	3
1.3 สิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลในบริบทกฎหมายสิทธิมนุษยชนระหว่างประเทศ	4
1.4 สิทธิในความเป็นอยู่ส่วนตัวตามกรอบแนวคิด “สิทธิที่จะอยู่ตามลำพัง” (Right to be let alone)	9
1.5 สิทธิในความเป็นอยู่ส่วนตัวตามกรอบแนวคิด “ระยะห่างระหว่างบุคคล” (Proxemics)	11
1.6 สิทธิในความเป็นอยู่ส่วนตัวตามกรอบแนวคิด “การจำกัดการเข้าถึง” (Limited-access theory)	13
1.7 สิทธิในความเป็นอยู่ส่วนตัวในแง่ “ความสันโดษหรือการแยกตัว” (Solitude)	14
1.8 สิทธิในความเป็นอยู่ส่วนตัวในแง่มุม “ความลับ” (Secrecy)	15
1.9 แนวคิดการจำแนก ขอบเขตสาธารณะ และ ขอบเขตส่วนบุคคล (Public and Private Sphere)	16
1.10 สิทธิในความเป็นอยู่ส่วนตัวในแง่ของ “การควบคุมข้อมูลส่วนบุคคล” (Control Theory) หรือ “ความเป็นส่วนตัวทางสารสนเทศ” (Information privacy)	20
1.11 สิทธิในความเป็นอยู่ส่วนตัวในแง่ของการกระทำที่เป็นภัยคุกคามความเป็นส่วนตัว	22
1.12 สิทธิในความเป็นอยู่ส่วนตัวกับการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์หรือสารสนเทศ (Privacy and Computer or Information Security)	23
1.13 สิทธิในความเป็นอยู่ส่วนตัวกับการรักษาความมั่นคงปลอดภัยของชาติหรือของรัฐ (Privacy and National or State Security)	28

1.14 การคุ้มครองข้อมูลส่วนบุคคลกับแนวคิด “คุณภาพของข้อมูลหรือคุณภาพทางสารสนเทศ” (Data Quality)	31
1.15 การคุ้มครองข้อมูลส่วนบุคคลกับแนวคิดการกำกับดูแลข้อมูล (Data Governance)	33
1.16 ลักษณะสำคัญของสิทธิในความเป็นส่วนตัว	35
1.17 สรุปเปรียบเทียบหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกรอบแนวคิดทฤษฎี	36
บทที่ 2 โครงสร้างและขอบเขตกฎหมายคุ้มครองข้อมูลส่วนบุคคล	39
2.1 โครงสร้างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	39
2.2 เปรียบเทียบบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกับหลักกฎหมายสหภาพยุโรป	41
2.3 ขอบเขตในแง่ความเป็นกฎหมายกลาง	49
2.4 ขอบเขตเชิงสาระ (Material scope)	50
2.4.1 ประโยชน์ส่วนตัวหรือกิจกรรมในครอบครัว	52
2.4.2 หน่วยงานรัฐเกี่ยวกับความมั่นคง	53
2.4.3 กิจกรรมสื่อมวลชน ศิลปกรรม วรรณกรรม	58
2.4.4 การดำเนินการของฝ่ายนิติบัญญัติ	59
2.4.5 การดำเนินการของฝ่ายตุลาการ	60
2.4.6 การดำเนินการตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต	60
2.4.7 การยกเว้นตามมาตรา 4 วรรคสอง	63
2.4.8 ผลของการยกเว้นตามมาตรา 4	63
2.5 ขอบเขตด้านพื้นที่ (Territorial scope)	64
2.5.1 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลอยู่ในราชอาณาจักร	64
2.5.2 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลอยู่นอกราชอาณาจักร	65
2.6 ขอบเขตด้านระยะเวลาการมีผลใช้บังคับของกฎหมาย	67

2.7 การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้	73
บทที่ 3 ข้อมูลส่วนบุคคลและการกระทำที่เกี่ยวข้อกับข้อมูลส่วนบุคคล	79
3.1 ข้อมูลส่วนบุคคล	79
3.1.1 นิยามและองค์ประกอบของข้อมูลส่วนบุคคล	79
3.1.2 การจำแนกประเภทข้อมูลส่วนบุคคล	85
3.1.3 ข้อมูลส่วนบุคคลกับข้อมูลที่ได้รับการคุ้มครองตามกฎหมายอื่น	88
3.1.4 ข้อมูลส่วนบุคคลกับข้อมูลสารสนเทศอื่นที่เกี่ยวข้องกับ การบริหารจัดการองค์กรหรือธุรกิจ	89
3.1.5 ข้อมูลนิรนาม (Anonymized data)	90
3.1.6 การแยกข้อมูลเพิ่มเติมออกไปเพื่อให้ไม่สามารถระบุตัวได้ (Pseudonymisation)	92
3.2 การกระทำ หรือ กิจกรรมเกี่ยวกับข้อมูลส่วนบุคคล ที่อยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล	93
3.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล (Collection)	94
3.2.2 การใช้ข้อมูลส่วนบุคคล (Use)	95
3.2.3 การเปิดเผยข้อมูลส่วนบุคคล (Disclosure or dissemination)	96
3.2.4 การกระทำอื่นที่กระทบต่อสิทธิในความเป็นส่วนตัว	98
บทที่ 4 บุคคลและองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และภาพรวมของหน้าที่ตามกฎหมาย	101
4.1 บุคคลหรือองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	101
4.1.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)	102
4.1.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Data Controller)	105
4.1.3 ผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controllers)	108
4.1.4 ผู้ประมวลผลข้อมูลส่วนบุคคล (Personal Data Processor)	110

4.1.5 บุคคลหรือนิติบุคคลที่มีหลายสถานะ	115
4.1.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	116
4.1.6.1 เจื่อนไขในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	116
4.1.6.2 ที่มาและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	118
4.1.6.3 การคุ้มครองการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล	120
4.1.6.4 หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูล ส่วนบุคคล	121
4.1.6.5 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกับบทบาทในการ ประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (DPIA)	123
4.2 ภาพรวมของหน้าที่และกรอบการปฏิบัติให้สอดคล้องกับกฎหมาย (Compliance)	124
4.2.1 ภาพรวมของหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล	124
4.2.2 กรอบการจัดเตรียมเอกสารหรือกระบวนการให้สอดคล้องกับ กฎหมายคุ้มครองข้อมูลส่วนบุคคล	129
บทที่ 5 ฐานหรือเหตุทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผยข้อมูล ส่วนบุคคล	138
5.1 ภาพรวมของฐานหรือเหตุทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล	138
5.2 ฐานความยินยอม (Consent)	142
5.2.1 การกระทำในเชิงยืนยันอันบ่งชี้เจตนาของเจ้าของข้อมูล อย่างไม่คลุมเครือ	143
5.2.1.1 รูปแบบหรือช่องทางการขอความยินยอม	143
5.2.1.2 การกระทำเชิงยืนยันอันชัดแจ้ง	144
5.2.1.3 เวลาในการขอความยินยอม	146
5.2.2 ความเป็นอิสระในการให้ความยินยอม (Freely given)	146

5.2.2.1 หลักทั่วไปของความเป็นอิสระในการให้ความยินยอม	147
5.2.2.2 ความไม่สมดุลเชิงอำนาจต่อรอง (Imbalance of power)	147
5.2.2.3 การสร้างเงื่อนไข (Conditionality)	150
5.2.2.4 ความยินยอมสำหรับการประมวลผลข้อมูลที่มีวัตถุประสงค์ หลายอย่าง (Granularity)	156
5.2.2.5 ผลกระทบทางลบจากการไม่ยินยอม	157
5.2.3 การแจ้งวัตถุประสงค์ในการขอความยินยอม (Informed consent)	158
5.2.4 ความเฉพาะเจาะจงของความยินยอม (Specific)	161
5.2.5 การขอความยินยอมในรูปแบบที่เข้าถึงง่ายและเข้าใจง่าย	163
5.2.6 ผลของความยินยอมที่ไม่สอดคล้องกับเงื่อนไขของกฎหมาย	164
5.2.6.1 กรณีศึกษาคำวินิจฉัยคณะกรรมการคุ้มครองข้อมูล ส่วนบุคคล ฝรั่งเศส	165
5.2.7 การถอนความยินยอม	166
5.2.8 การขอความยินยอมสำหรับผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ	169
5.2.9 กรณีศึกษา ความยินยอม สำหรับแอปพลิเคชัน “หมอชนะ”	175
5.3 ฐานปฏิบัติตามสัญญาหรือดำเนินการตามคำขอก่อนเข้าทำสัญญา (Necessary for performance of a contract)	177
5.3.1 การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลเพื่อการปฏิบัติตาม สัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา	178
5.3.2 ความจำเป็นเพื่อดำเนินการตามคำขอของเจ้าของข้อมูล ส่วนบุคคลก่อนเข้าทำสัญญา	182
5.3.3 ความจำเป็นเพื่อประโยชน์อื่นในทางธุรกิจของผู้ควบคุมข้อมูล ซึ่งนำมาผนวกไว้ในข้อสัญญา	183
5.4 ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)	185
5.4.1 ตัวอย่างกฎหมายอื่นที่กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล	186
5.4.2 กรณีศึกษา : การเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลเพื่อ ควบคุมโรคติดต่อโควิด-19	193

5.4.3 เปรียบเทียบ มาตรา 24 (6) กับ มาตรา 4 (2)	196
5.5 ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ ของบุคคล (Vital interest)	197
5.6 ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public task)	199
5.7 ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate interest)	201
5.7.1 บุคคลที่สามารถอ้างประโยชน์โดยชอบด้วยกฎหมาย	201
5.7.2 เงื่อนไขในการอ้างฐานประโยชน์โดยชอบด้วยกฎหมายของผู้ ควบคุมข้อมูลส่วนบุคคล	202
5.7.3 เกณฑ์การชั่งน้ำหนักประโยชน์โดยชอบด้วยกฎหมาย	204
5.7.4 การอ้างฐานประโยชน์โดยชอบด้วยกฎหมายที่กว้างเกินไป	208
5.7.5 กิจกรรมที่มีหลายวัตถุประสงค์	210
5.8 ฐานการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์ สาธารณะหรือการศึกษาวิจัย	211
5.9 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	213

บทที่ 6 ฐานหรือเหตุทางกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคล ชนิดพิเศษ	222
6.1 หลักการ ขอบเขตของข้อมูลส่วนบุคคลตามมาตรา 26 และภาพรวมของฐานหรือเหตุทางกฎหมาย	222
6.2 ฐานความยินยอมโดยชัดแจ้ง (Explicit consent)	228
6.2.1 เงื่อนไขของความยินยอมโดยชัดแจ้ง	228
6.2.2 การนำข้อมูลส่วนบุคคลชนิดพิเศษเป็นเงื่อนไขในการให้บริการ	231
6.3 ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการจ้างแรงงาน และความคุ้มครองทางสังคม	232
6.4 ฐานประโยชน์สำคัญต่อชีวิต (Vital interest)	234
6.5 ฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือ องค์กรไม่แสวงหากำไร	236

6.6	ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง จากเจ้าของข้อมูลส่วนบุคคล	237
6.7	ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับการใช้สิทธิเรียกร้อง ตามกฎหมาย	238
6.8	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะ ที่สำคัญ	240
6.9	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการให้บริการ ด้านสุขภาพหรือสังคม	242
6.10	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะ ด้านสาธารณสุข	244
6.11	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัย ทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ	245
6.12	ข้อมูลชีวภาพ (Biometric data)	247
6.12.1	กรณีศึกษา การเก็บรวบรวมข้อมูลภาพจำลองใบหน้าประชาชน โดยหน่วยงานบังคับใช้กฎหมาย	249
6.13	ข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม	252
6.14	กรณีศึกษาคดีเกี่ยวกับผลกระทบต่อสิทธิขั้นพื้นฐานของข้อมูล ส่วนบุคคลชนิดพิเศษและหน้าที่อื่นของผู้ควบคุมข้อมูลส่วนบุคคล ชนิดพิเศษ	254
6.15	กรณีศึกษาคดีเกี่ยวกับข้อมูลส่วนบุคคลชนิดพิเศษในสภาพแวดล้อม การสื่อสารออนไลน์	255

บทที่ 7	หลักกฎหมายเกี่ยวกับ “วัตถุประสงค์” และการแจ้งรายละเอียด ให้เจ้าของข้อมูลทราบ (Privacy information or Privacy Notice)	259
7.1	หลักพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ “วัตถุประสงค์” และความสัมพันธ์กับบทมาตรต่างๆ	259
7.2	การแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Privacy information หรือ Privacy Notice)	262
7.2.1	เปรียบเทียบหลักกฎหมายสหภาพยุโรปและกฎหมายไทย	263

7.2.1.1 การแจ้งรายละเอียดในกรณีเก็บรวบรวมข้อมูลส่วนบุคคลจาก เจ้าของข้อมูล (Personal data are collected from the data subject)	263
7.2.1.2 การแจ้งรายละเอียดในกรณีเก็บรวบรวมจากแหล่งอื่นที่ ไม่ใช่เจ้าของข้อมูล (Personal data have not been obtained from the data subject)	264
7.2.1.3 ตารางเปรียบเทียบรายละเอียดที่ต้องแจ้งให้เจ้าของข้อมูลทราบ (Privacy information / Privacy notice) ตามกฎหมาย สหภาพยุโรปและกฎหมายไทย	268
7.2.2 รายการที่ต้องแจ้งให้เจ้าของข้อมูลทราบ (Privacy information or notice)	271
7.2.3 รูปแบบและวิธีการแจ้ง	280
7.2.3.1 เงื่อนไขของการร่างเนื้อหาที่ต้องแจ้ง	280
7.2.3.2 วิธีการและเทคนิคในการแจ้ง	281
7.2.3.3 การตอบสนองหรือตอบรับจากเจ้าของข้อมูลส่วนบุคคล	282
7.2.3.4 กรณีศึกษา	283
7.2.4 การแจ้งให้ทราบกับการขอความยินยอม	284
7.2.4.1 กรณีศึกษา การแจ้งรายละเอียด (Privacy notice / information) และการขอความยินยอมของผู้ให้บริการเว็บไซต์ ที่ใช้คุกกี้	286
7.2.5 ระยะเวลาการแจ้ง	289
7.2.6 ผู้ประมวลผลข้อมูลส่วนบุคคล กับ การแจ้งรายละเอียด (Privacy information or Privacy Notice)	291
7.2.7 ข้อยกเว้นของการแจ้งรายละเอียด (Privacy information)	292
7.2.7.1 กรณีเก็บรวบรวมข้อมูลจากเจ้าของข้อมูล	292
7.2.7.2 กรณีเก็บรวบรวมข้อมูลจากแหล่งอื่น	293
7.2.8 ตัวอย่างการแจ้งรายละเอียดในรูปแบบ “นโยบายคุ้มครองข้อมูล ส่วนบุคคล” (Privacy policy)	295

7.3 การกระทำต่อข้อมูลส่วนบุคคลเพิ่มเติมหรือแตกต่างจากวัตถุประสงค์ ที่แจ้งไว้ (Further processing of personal data)	300
---	-----

บทที่ 8 หลักกฎหมายเกี่ยวกับมาตรฐานและคุณภาพของข้อมูลส่วนบุคคล	308
--	------------

8.1 หลักการประมวลข้อมูลที่น้อยที่สุดเท่าที่จำเป็น (Data minimization)	308
8.1.1 การเก็บรวบรวมข้อมูลน้อยเกินไปอาจไม่สอดคล้องกับหลักการ ประมวลข้อมูลที่น้อยที่สุด	310
8.1.2 การเก็บรวบรวมข้อมูลเพื่อวัตถุประสงค์บางประการในอนาคต	311
8.1.3 การเก็บข้อมูลเพื่อรองรับการดำเนินการในอนาคตที่ไม่เกี่ยวกับ วัตถุประสงค์ในขั้นตอนการเก็บรวบรวมข้อมูล	312
8.1.4 การเก็บรวบรวมข้อมูลเพื่อวัตถุประสงค์ที่ประกอบด้วยกิจกรรมย่อย หลายขั้นตอน	313
8.1.5 การเก็บรวบรวมข้อมูลส่วนบุคคลบางอย่างที่มีข้อมูลย่อย หรือรายละเอียดหลายส่วน	314
8.1.6 การเก็บข้อมูลเท่าที่จำเป็นเพื่อวัตถุประสงค์ในการยืนยันตัวตน	315
8.1.7 หลักความได้สัดส่วนและทางเลือกอื่นที่จำกัดสิทธิน้อยกว่า	318
8.2 หลักการเก็บรักษาข้อมูลอย่างจำกัด (Storage limitation)	320
8.2.1 ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล	320
8.2.2 ระยะเวลาเก็บรักษา กับฐานหรือเหตุ (Lawful basis)	321
8.2.3 การเก็บรักษาข้อมูลเมื่อความสัมพันธ์กับเจ้าของข้อมูลสิ้นสุดลง	322
8.2.4 ข้อควรระวังในการเก็บรักษาข้อมูลส่วนบุคคล	322
8.2.5 ระยะเวลาเก็บรักษาในกรณีผู้ประมวลผลข้อมูลส่วนบุคคล	324
8.2.6 ระยะเวลาเก็บรักษา กับ สิทธิของเจ้าของข้อมูล	324
8.2.7 ความสัมพันธ์ของหลักการประมวลข้อมูลที่น้อยที่สุดเท่าที่จำเป็น และหลักการเก็บรักษาข้อมูลอย่างจำกัด	325
8.3 หลักความถูกต้อง (Accuracy)	327

8.3.1 ความถูกต้อง ประกอบด้วยคุณลักษณะด้านคุณภาพ หรือมาตรฐานหลายประการ	328
8.3.2 ข้อมูลที่เป็นปัจจุบัน (Up to date)	328
8.3.3 ข้อมูลที่ผิดพลาด (Mistake) และข้อมูลที่ทำให้เกิดความเข้าใจผิด (Misleading)	330
8.3.4 ความถูกต้องของข้อมูลส่วนบุคคลที่เป็นความคิดเห็น	331
8.4 โทษของการฝ่าฝืนหลักกฎหมายเกี่ยวกับมาตรฐานและคุณภาพ ของข้อมูลส่วนบุคคล	331

บทที่ 9 หน้าที่การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ส่วนบุคคล	333
9.1 ภาพรวมของหลักกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคง ปลอดภัยของข้อมูลส่วนบุคคล	334
9.2 ภัยคุกคามความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือการละเมิด ข้อมูลส่วนบุคคล	335
9.2.1 กรอบแนวคิดเกี่ยวกับเกณฑ์จำแนกภัยคุกคามทางคอมพิวเตอร์	336
9.2.2 ภัยคุกคามความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือ การละเมิดข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	338
9.2.2.1 ภัยคุกคามข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วน บุคคลสหภาพยุโรป (GDPR)	338
9.2.2.2 ภัยคุกคามข้อมูลส่วนบุคคลหรือการละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	339
9.2.3 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาจากผู้ก่อภัยคุกคาม	342
9.2.3.1 การจำแนกภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาความสัมพันธ์ระหว่างผู้ก่อภัยคุกคามและผู้ควบคุม ข้อมูลส่วนบุคคล	342
9.2.3.2 การจำแนกภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคลโดย พิจารณาเจตนาของผู้ก่อภัยคุกคาม	343

9.2.4 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาวิธีการและเป้าหมาย	345
9.2.5 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล ที่ไม่ได้เกิดจากการกระทำของบุคคล	345
9.2.6 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยคุณลักษณะด้านความปลอดภัยทางคอมพิวเตอร์	346
9.2.7 ภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคลกับอาชญากรรม คอมพิวเตอร์ในกรอบพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์	348
9.2.8 หน้าที่และความรับผิดชอบตามกฎหมายของผู้เกี่ยวข้องกับภัยคุกคาม หรือการละเมิดข้อมูลส่วนบุคคล	352
9.2.9 ผลกระทบจากภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล	355
9.3 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	358
9.3.1 รายละเอียดตามกฎหมายของมาตรการหรือมาตรฐานการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	358
9.3.1.1 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563	359
9.3.1.2 มาตรการหรือมาตรฐานการรักษาความมั่นคงปลอดภัยของ ข้อมูลส่วนบุคคลตาม GDPR	363
9.3.2 บุคคลที่ต้องรับผิดชอบและประเด็นเกี่ยวกับเจตนา	365
9.3.3 ปัจจัยในการพิจารณา “ความเหมาะสม” ของมาตรการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	366
9.3.4 ปัจจัยเกี่ยวความเสี่ยง (Risk) ของผลกระทบหรือความเสียหาย ต่อเจ้าของข้อมูลส่วนบุคคล	368
9.3.5 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลด้านต่างๆ	369
9.4 กรณีศึกษาในทางคดีเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล	372
9.5 กรอบแนวทางการร่างนโยบายรักษาความมั่นคงปลอดภัยของข้อมูล ส่วนบุคคล	378

9.6 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal data breach notification)	389
9.6.1 เหตุผลของการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	389
9.6.2 ผู้มีหน้าที่แจ้งและผู้รับการแจ้ง	389
9.6.3 เงื่อนไขและข้อยกเว้นของการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	391
9.6.4 เนื้อหาหรือรายละเอียดที่ต้องแจ้ง	393

บทที่ 10 หน้าที่ตามกฎหมายและความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล	395
10.1 หลักกฎหมายที่เกี่ยวข้องกับความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล	395
10.2 เงื่อนไขเบื้องต้นในการพิจารณาความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล	400
10.3 สัญญาที่เกี่ยวข้องในความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับผู้ประมวลผลข้อมูลส่วนบุคคล	401
10.4 ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลหรือสัญญาประมวลผลข้อมูลส่วนบุคคล	403
10.4.1 แนวทางการร่างสัญญาประมวลผลข้อมูลส่วนบุคคลและเปรียบเทียบกับกฎหมายสหภาพยุโรป	404
10.4.2 ส่วนของชื่อและคู่สัญญา	406
10.4.3 อาร์ัมบทหรือเกริ่นนำ (Preamble)	406
10.4.4 นิยาม (Definition)	408
10.4.5 สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	409
10.4.6 คำสั่งของผู้ควบคุมข้อมูลต่อผู้ประมวลผลและข้อกำหนดห้ามมิให้ผู้ประมวลผลทำการนอกเหนือจากคำสั่ง	410
10.4.7 ข้อสัญญาเกี่ยวกับหน้าที่รักษาความลับ (Duty of confidence)	411
10.4.8 ข้อสัญญาเกี่ยวกับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล	413
10.4.9 ข้อสัญญาเกี่ยวกับผู้ประมวลผลช่วง (Sub-processor)	415

10.4.10 ข้อสัญญากำหนดหน้าที่ผู้ประมวลผลในการช่วยเหลือผู้ควบคุมข้อมูลให้ปฏิบัติหน้าที่ตามกฎหมาย	417
10.4.11 ข้อสัญญาเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	418
10.4.12 ข้อสัญญาเกี่ยวกับการลบหรือส่งคืนข้อมูลส่วนบุคคล	419

บทที่ 11 สิทธิเจ้าของข้อมูล 421

11.1 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access)	422
11.2 สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to rectification)	430
11.3 สิทธิในการขอให้ลบข้อมูลส่วนบุคคล (Right to erasure) หรือ สิทธิที่จะถูกลืม (Right to be forgotten)	431
11.3.1 สิทธิที่จะถูกลืมตามกฎหมายสหภาพยุโรปก่อน GDPR	432
11.3.2 เปรียบเทียบสิทธิที่จะถูกลืมตาม GDPR กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	434
11.3.2.1 หลักทั่วไปของสิทธิที่จะถูกลืม	434
11.3.2.2 เหตุแห่งการใช้สิทธิในการลบข้อมูลส่วนบุคคล	435
11.3.2.3 ข้อยกเว้นหรือข้อจำกัดสิทธิในการลบข้อมูลส่วนบุคคล	437
11.3.3 เปรียบเทียบคำพิพากษาศาลยุโรปกับสิทธิในการลบข้อมูลส่วนบุคคลตามกฎหมายไทย	438
11.3.4 สิทธิที่จะถูกลืม เปรียบเทียบกับการลบหรือทำลายข้อมูลตามกฎหมายอื่น	443
11.4 สิทธิในการคัดค้านการประมวลข้อมูลส่วนบุคคล (Right to object)	445
11.4.1 เงื่อนไขและข้อจำกัดสิทธิคัดค้าน	445
11.4.2 การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล	448
11.5 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing)	448
11.5.1 เงื่อนไขของการใช้สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล	448
11.5.2 การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล	451

11.6 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability)	451
11.7 สิทธิในการได้รับแจ้งข้อมูลหรือรายละเอียดเกี่ยวกับการประมวลผล ข้อมูลส่วนบุคคล (Right to be informed)	455
11.8 ประเด็นพิจารณาเกี่ยวกับสิทธิของเจ้าของข้อมูล	456
11.8.1 รูปแบบและวิธีการร้องขอใช้สิทธิ	456
11.8.2 การบันทึกรายการเกี่ยวกับสิทธิของเจ้าของข้อมูล	460
11.8.3 ค่าธรรมเนียมของการใช้สิทธิ	462
11.8.4 การสร้างเงื่อนไขของการใช้สิทธิที่เป็นอุปสรรคต่อเจ้าของข้อมูล	463
11.9 ความสัมพันธ์ระหว่าง สิทธิของเจ้าของข้อมูลกับเหตุหรือฐาน ทางกฎหมาย	464
บทที่ 12 ความรับผิด โทษ และการร้องเรียน	468
12.1 ความรับผิดและโทษของผู้ควบคุมข้อมูลส่วนบุคคล	468
12.2 ความรับผิดและโทษของผู้ประมวลผลข้อมูลส่วนบุคคล	482
12.3 ความรับผิดและโทษสำหรับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผล	485
12.4 ความรับผิดและโทษที่ไม่จำกัดสถานะของบุคคล	486
12.5 การร้องเรียน	487
12.5.1 การร้องเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	487
12.5.2 เปรียบเทียบการร้องเรียนตามกฎหมายสหภาพยุโรป	491
บทส่งท้าย ข้อจำกัดและผลกระทบทางลบของกฎหมายคุ้มครองข้อมูล ส่วนบุคคล	495

บรรณานุกรม	521
ภาคผนวก	
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	538
- พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคล ไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563	585
- ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการ ผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓	589
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓	592
ประวัติผู้เขียน	594

สำหรับเพื่อการศึกษาและอ้างอิงเท่านั้น
For educational use and reference only