



คำอธิบาย หลักกฎหมาย คุ้มครองข้อมูลส่วนบุคคล



รองศาสตราจารย์ **คนาริป ทองรวีวงศ์**
คณะนิติศาสตร์ และสถาบันกฎหมายสื่อดิจิทัล
มหาวิทยาลัยเกษมบัณฑิต

สารบัญ

บทที่ 1 กรอบแนวคิด ทฤษฎี ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	1
1.1 ความหมายทั่วไปของความเป็นอยู่ส่วนตัว	2
1.2 ความเป็นอยู่ส่วนตัวในแง่ของสิทธิ	3
1.3 สิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลในบริบทกฎหมายสิทธิ มนุษยชนระหว่างประเทศ	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 แนวคิดการจำแนกขอบเขตสาธารณะและขอบเขตส่วนบุคคล (Public and Private Sphere)	16
1.10 สิทธิในความเป็นอยู่ส่วนตัวในแง่ของ “การควบคุมข้อมูลส่วนบุคคล” (Control Theory) หรือ “ความเป็นส่วนตัวทางสารสนเทศ” (Information privacy)	20
1.11 สิทธิในความเป็นอยู่ส่วนตัวในแง่ของการกระทำที่เป็นภัยคุกคาม ความเป็นส่วนตัว	22
1.12 สิทธิในความเป็นอยู่ส่วนตัวกับการรักษาความมั่นคงปลอดภัย ทางคอมพิวเตอร์หรือสารสนเทศ (Privacy and Computer or Information Security)	23
1.13 สิทธิในความเป็นอยู่ส่วนตัวกับการรักษาความมั่นคงปลอดภัย ของชาติหรือของรัฐ (Privacy and National or State Security)	28

1.14 การคุ้มครองข้อมูลส่วนบุคคลกับแนวคิด “คุณภาพของข้อมูลหรือคุณภาพทางสารสนเทศ” (Data Quality)	31
1.15 การคุ้มครองข้อมูลส่วนบุคคลกับแนวคิดการกำกับดูแลข้อมูล (Data Governance)	33
1.16 ลักษณะสำคัญของสิทธิในความเป็นอยู่ส่วนตัว	35
1.17 กรณีศึกษาความแตกต่างเชิงขอบเขตของสิทธิในความเป็นอยู่ส่วนตัว และข้อมูลส่วนบุคคลจากคำพิพากษาศาลในสหภาพยุโรป	36
1.18 สรุปเปรียบเทียบหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกรอบแนวคิดทฤษฎี	38
บทที่ 2 โครงสร้างและขอบเขตกฎหมายคุ้มครองข้อมูลส่วนบุคคล	41
2.1 โครงสร้างของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	41
2.2 เปรียบเทียบบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกับหลักกฎหมายสหภาพยุโรป	43
2.3 ขอบเขตในแง่ความเป็นกฎหมายกลาง	51
2.4 ขอบเขตเชิงสาระ (Material scope)	58
2.4.1 ประโยชน์ส่วนตนหรือกิจกรรมในครอบครัว	61
2.4.1.1 ขอบเขตในแง่พื้นที่ของกิจกรรมเพื่อประโยชน์ส่วนตัวหรือในครอบครัว	64
2.4.2 หน่วยงานรัฐเกี่ยวกับความมั่นคง	71
2.4.2.1 กฎหมายเกี่ยวกับความมั่นคงที่ให้อำนาจหน่วยงานรัฐเก็บรวบรวมข้อมูลส่วนบุคคล	72
2.4.2.2 กรณีศึกษา การตีความขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับหน่วยงานรัฐที่ดำเนินการด้านภาษีอากร	77
2.4.3 กิจการสื่อมวลชน ศิลปกรรม วรรณกรรม	82
2.4.4 การดำเนินการของฝ่ายนิติบัญญัติ	89
2.4.5 การดำเนินการของฝ่ายตุลาการ	90

2.4.6 การดำเนินการตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต	93
2.4.7 การยกเว้นตามมาตรา 4 วรรคสอง และพระราชกฤษฎีกาที่เกี่ยวข้อง	95
2.4.8 ผลของการยกเว้นตามมาตรา 4	104
2.5 ขอบเขตด้านพื้นที่ (Territorial scope)	105
2.5.1 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลอยู่ในราชอาณาจักร	105
2.5.2 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลอยู่นอกราชอาณาจักร	106
2.6 ขอบเขตด้านระยะเวลาการมีผลใช้บังคับของกฎหมาย	108
2.7 การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้	115

บทที่ 3 ข้อมูลส่วนบุคคลและการกระทำเกี่ยวกับข้อมูลส่วนบุคคล	121
3.1 ข้อมูลส่วนบุคคล	121
3.1.1 นิยามและองค์ประกอบของข้อมูลส่วนบุคคล	121
3.1.2 การจำแนกประเภทข้อมูลส่วนบุคคล	127
3.1.3 ข้อมูลส่วนบุคคลกับข้อมูลที่ได้รับการคุ้มครองตามกฎหมายอื่น	130
3.1.4 ข้อมูลส่วนบุคคลกับข้อมูลสารสนเทศอื่นที่เกี่ยวข้องกับการบริหารจัดการองค์กรหรือธุรกิจ	131
3.1.5 ข้อมูลนิรนาม (Anonymized data)	132
3.1.6 การแยกข้อมูลเพิ่มเติมออกไปเพื่อให้ไม่สามารถระบุตัวได้ (Pseudonymisation)	134
3.2 การกระทำหรือกิจกรรมเกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล	135
3.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล (Collection)	136
3.2.2 การใช้ข้อมูลส่วนบุคคล (Use)	137
3.2.3 การเปิดเผยข้อมูลส่วนบุคคล (Disclosure or dissemination)	138
3.2.4 การกระทำอื่นที่กระทบต่อสิทธิในความเป็นอยู่ส่วนตัว	140

บทที่ 4 บุคคลและองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	
และภาพรวมของหน้าที่ตามกฎหมาย	143
4.1 บุคคลหรือองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	143
4.1.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)	144
4.1.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Data Controller)	147
4.1.3 ผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controllers)	152
4.1.4 ผู้ประมวลผลข้อมูลส่วนบุคคล (Personal Data Processor)	155
4.1.5 บุคคลหรือนิติบุคคลที่มีหลายสถานะ	159
4.1.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	160
4.1.6.1 เงื่อนไขในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	160
4.1.6.2 ที่มาและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	163
4.1.6.3 การคุ้มครองการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	164
4.1.6.4 หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	165
4.1.6.5 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกับบทบาทในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (DPIA)	167
4.1.7 ลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล	169
4.2 ภาพรวมของหน้าที่และกรอบการปฏิบัติให้สอดคล้องกับกฎหมาย (Compliance)	170
4.2.1 ภาพรวมของหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล	170
4.2.2 กรอบการจัดเตรียมเอกสารหรือกระบวนการให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	177

บทที่ 5 ฐานหรือเหตุทางกฎหมายในการเก็บ รวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล	186
5.1 ภาพรวมของฐานหรือเหตุทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล	186
5.2 ฐานความยินยอม (Consent)	190
5.2.1 การกระทำในเชิงยืนยันอันพึงชี้เจตนาของเจ้าของข้อมูลอย่างไม่คลุมเครือ	191
5.2.1.1 รูปแบบหรือช่องทางการขอความยินยอม	191
5.2.1.2 การกระทำเชิงยืนยันอันชัดแจ้ง	192
5.2.1.3 เวลาในการขอความยินยอม	194
5.2.2 ความเป็นอิสระในการให้ความยินยอม (Freely given)	194
5.2.2.1 หลักทั่วไปของความเป็นอิสระในการให้ความยินยอม	195
5.2.2.2 ความไม่สมดุลเชิงอำนาจต่อรอง (Imbalance of power)	195
5.2.2.3 การสร้างเงื่อนไข (Conditionality)	198
5.2.2.4 ความยินยอมสำหรับการประมวลผลข้อมูลที่มีวัตถุประสงค์หลายอย่าง (Granularity)	204
5.2.2.5 ผลกระทบทางลบจากการไม่ยินยอม	205
5.2.2.6 กรณีศึกษา การขอความยินยอมเพื่อนำข้อมูลที่ได้จากโครงการหรือกิจกรรมหนึ่งไปต่อยอดหรือบูรณาการกับโครงการหรือกิจกรรมอื่น	207
5.2.3 การแจ้งวัตถุประสงค์ในการขอความยินยอม (Informed consent)	208
5.2.4 ความเฉพาะเจาะจงของความยินยอม (Specific)	211
5.2.5 การขอความยินยอมในรูปแบบที่เข้าถึงง่ายและเข้าใจง่าย	213
5.2.6 ผลของความยินยอมที่ไม่สอดคล้องกับเงื่อนไขของกฎหมาย	214
5.2.6.1 กรณีศึกษาคำวินิจฉัยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฝรั่งเศส	215
5.2.7 การถอนความยินยอม	216

5.2.8 การขอความยินยอมสำหรับผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ	219
5.2.9 กรณีศึกษา ความยินยอมที่เกี่ยวข้องกับมาตรการรัฐในการ ควบคุมโรคติดต่อโควิด 19	225
5.2.9.1 กรณีศึกษา วิเคราะห์ความยินยอมของผู้ใช้งาน “แอปพลิเคชันที่ทางราชการกำหนด”	226
5.2.9.1.1 ความยินยอมของผู้ใช้งาน “แอปพลิเคชันหมอชนะ”	228
5.2.9.1.2 ความยินยอมของผู้ใช้งาน “แอปพลิเคชันไทยชนะ”	234
5.2.9.2 กรณีศึกษา วิเคราะห์ความยินยอมของผู้ใช้งานแพลตฟอร์ม การเข้าถึงวัคซีนป้องกันโรคติดต่อโควิด-19	240
5.2.9.2.1 ความยินยอมข้อมูลส่วนบุคคลตามข้อตกลง “ไทยร่วมใจ”	240
5.2.10 กรณีศึกษา การเลือกใช้ฐานความยินยอมกับการเก็บรวบรวมข้อมูล ส่วนบุคคลที่อาจเข้าองค์ประกอบมากกว่าหนึ่งฐานทางกฎหมาย : ลำดับและการสืบเปลี่ยนการอ้างฐานทางกฎหมาย	245
5.2.11 กรณีศึกษา ความยินยอมหลายมิติในบริบทความสัมพันธ์ของ ผู้ควบคุมข้อมูลส่วนบุคคลหลายราย	247
5.3 ฐานปฏิบัติตามสัญญาหรือดำเนินการตามคำขอก่อนเข้าทำสัญญา (Necessary for performance of a contract)	250
5.3.1 การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลเพื่อปฏิบัติ ตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา	250
5.3.1.1 การนำเสนอสินค้าหรือบริการประเภทเดียวกันหรือเกี่ยวเนื่อง กับสินค้าหรือบริการเดิม กับการอ้างฐานปฏิบัติตามสัญญา	254
5.3.2 ความจำเป็นเพื่อดำเนินการตามคำขอของเจ้าของข้อมูล ส่วนบุคคลก่อนเข้าทำสัญญา	256
5.3.3 ความจำเป็นเพื่อประโยชน์อื่นในทางธุรกิจของผู้ควบคุมข้อมูล ซึ่งนำมาผนวกไว้ในข้อสัญญา	257
5.3.4 กรณีศึกษา กลยุทธ์หลีกเลี่ยงการขอความยินยอมมาใช้ฐานสัญญา ที่ผู้บริโภคจำเป็นต้องยอมรับ	259

5.4 ฐานการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation)	262
5.4.1 ตัวอย่างกฎหมายอื่นที่กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล	262
5.4.1.1 กรณีศึกษา : การปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ตามพระราชกำหนดมาตรการป้องกันและปราบปราม อาชญากรรมทางเทคโนโลยี พ.ศ. 2566	269
5.4.2 กรณีศึกษา : การเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคล ตามมาตรการควบคุมโรคติดต่อโควิด-19	275
5.4.2.1 กรณีศึกษา ข้อตกลงและเงื่อนไขของแพลตฟอร์มหมอพร้อม	275
5.4.2.2 กรณีศึกษา ฐานทางกฎหมายที่เกี่ยวข้องกับแอปพลิเคชันเพื่อ ป้องกันโรคติดต่อโควิด 19 ของประเทศนอร์เวย์	287
5.4.3 เปรียบเทียบ มาตรา 24 (6) กับ มาตรา 4 (2)	292
5.5 ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ ของบุคคล (Vital interest)	293
5.6 ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (Public task)	295
5.7 ฐานประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate interest)	296
5.7.1 บุคคลที่สามารถอ้างประโยชน์โดยชอบด้วยกฎหมาย	297
5.7.2 เงื่อนไขในการอ้างฐานประโยชน์โดยชอบด้วยกฎหมายของ ผู้ควบคุมข้อมูลส่วนบุคคล	298
5.7.3 เกณฑ์การชั่งน้ำหนักประโยชน์โดยชอบด้วยกฎหมาย	299
5.7.4 การอ้างฐานประโยชน์โดยชอบด้วยกฎหมายที่กว้างเกินไป	303
5.7.5 กิจกรรมที่มีหลายวัตถุประสงค์	305
5.8 ฐานการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์ สาธารณะหรือการศึกษาวิจัย	307
5.9 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	308

บทที่ 6	ฐานหรือเหตุทางกฎหมายในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลชนิดพิเศษ	318
6.1	หลักการ ขอบเขตของข้อมูลส่วนบุคคลตามมาตรา 26 และภาพรวมของฐานหรือเหตุทางกฎหมาย	318
6.2	ฐานความยินยอมโดยชัดแจ้ง (Explicit consent)	324
6.2.1	เงื่อนไขของความยินยอมโดยชัดแจ้ง	324
6.2.2	การนำข้อมูลส่วนบุคคลชนิดพิเศษเป็นเงื่อนไขในการให้บริการ	327
6.3	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการจ้างแรงงาน และความคุ้มครองทางสังคม	328
6.4	ฐานประโยชน์สำคัญต่อชีวิต (Vital interest)	330
6.5	ฐานการดำเนินกิจกรรมของมูลนิธิ สมาคม หรือ องค์กรไม่แสวงหากำไร	332
6.6	ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง จากเจ้าของข้อมูลส่วนบุคคล	333
6.7	ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับการใช้สิทธิเรียกร้องตามกฎหมาย	334
6.8	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ	336
6.9	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับการให้บริการด้านสุขภาพหรือสังคม	338
6.10	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข	340
6.10.1	กรณีศึกษา กฎหมายเกี่ยวกับสาธารณสุขที่ระบุวัตถุประสงค์เพื่อประโยชน์สาธารณะอื่นหลายมิติ	341
6.11	ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติ	343
6.12	ข้อมูลชีวภาพ (Biometric data)	345
6.12.1	กรณีศึกษา การเก็บรวบรวมข้อมูลภาพจำลองใบหน้าประชาชนโดยหน่วยงานบังคับใช้กฎหมาย	347

6.12.2	กรณีศึกษา กฎหมายเฉพาะที่กำหนดให้เก็บรวบรวมข้อมูลชีวภาพ	350
6.12.2.1	การพิสูจน์ทราบตัวตนโดยข้อมูลชีวภาพตามกฎหมายป้องกันและปราบปรามการฟอกเงิน	351
6.12.2.2	กฎหมายและแนวปฏิบัติเกี่ยวกับการยืนยันและพิสูจน์ตัวตนของธนาคารแห่งประเทศไทย	355
6.13	ข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม	360
6.14	กรณีศึกษาคดีเกี่ยวกับผลกระทบต่อสิทธิขั้นพื้นฐานของข้อมูลส่วนบุคคลชนิดพิเศษและหน้าที่อื่นของผู้ควบคุมข้อมูลส่วนบุคคลชนิดพิเศษ	365
6.15	กรณีศึกษาคดีเกี่ยวกับข้อมูลส่วนบุคคลชนิดพิเศษในสภาพแวดล้อมการสื่อสารออนไลน์	367

บทที่ 7	หลักกฎหมายเกี่ยวกับ “วัตถุประสงค์” และการแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ (Privacy information or Privacy Notice)	370
7.1	หลักพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ “วัตถุประสงค์” และความสัมพันธ์กับบทมาตรต่างๆ	370
7.2	การแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล (Privacy information หรือ Privacy Notice)	373
7.2.1	เปรียบเทียบหลักกฎหมายสหภาพยุโรปและกฎหมายไทย	374
7.2.1.1	การแจ้งรายละเอียดในกรณีเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูล (Personal data are collected from the data subject)	374
7.2.1.2	การแจ้งรายละเอียดในกรณีเก็บรวบรวมจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูล (Personal data have not been obtained from the data subject)	375
7.2.1.3	ตารางเปรียบเทียบรายละเอียดที่ต้องแจ้งให้เจ้าของข้อมูลทราบ (Privacy information / Privacy notice) ตามกฎหมายสหภาพยุโรปและกฎหมายไทย	379
7.2.2	รายการที่ต้องแจ้งให้เจ้าของข้อมูลทราบ (Privacy information or notice)	382

7.2.3 รูปแบบและวิธีการแจ้ง	391	8.1.4 การเก็บรวบรวมเพื่อวัตถุประสงค์ที่ประกอบด้วยกิจกรรมย่อย หลายขั้นตอน	424
7.2.3.1 เงื่อนไขของการร่างเนื้อหาที่ต้องแจ้ง	391	8.1.5 การเก็บรวบรวมข้อมูลส่วนบุคคลบางอย่างที่มีข้อมูลย่อย หรือรายละเอียดหลายส่วน	425
7.2.3.2 วิธีการและเทคนิคในการแจ้ง	392	8.1.6 การเก็บข้อมูลเท่าที่จำเป็นเพื่อวัตถุประสงค์ในการยืนยันตัวตน	426
7.2.3.3 การตอบสนองหรือตอบรับจากเจ้าของข้อมูลส่วนบุคคล	393	8.1.7 หลักความได้สัดส่วนและทางเลือกอื่นที่จำกัดสิทธิน้อยกว่า	429
7.2.3.4 กรณีศึกษา	394	8.2 หลักการเก็บรักษาข้อมูลอย่างจำกัด (Storage limitation)	431
7.2.4 การแจ้งให้ทราบกับการขอความยินยอม	395	8.2.1 ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล	431
7.2.4.1 กรณีศึกษา การแจ้งรายละเอียด (Privacy notice / information) และการขอความยินยอมของผู้ให้บริการเว็บไซต์ ที่ใช้คุกกี้	397	8.2.2 ระยะเวลาเก็บรักษากับฐานหรือเหตุ (Lawful basis)	432
7.2.5 ระยะเวลาการแจ้ง	400	8.2.3 การเก็บรักษาข้อมูลเมื่อความสัมพันธ์กับเจ้าของข้อมูลสิ้นสุดลง	433
7.2.6 ผู้ประมวลผลข้อมูลส่วนบุคคลกับการแจ้งรายละเอียด (Privacy information or Privacy Notice)	402	8.2.4 ข้อยกเว้นในการเก็บรักษาข้อมูลส่วนบุคคล	433
7.2.7 ข้อยกเว้นของการแจ้งรายละเอียด (Privacy information)	402	8.2.5 ระยะเวลาเก็บรักษาในกรณีผู้ประมวลผลข้อมูลส่วนบุคคล	435
7.2.7.1 กรณีเก็บรวบรวมข้อมูลจากเจ้าของข้อมูล	403	8.2.6 ระยะเวลาเก็บรักษากับสิทธิของเจ้าของข้อมูล	435
7.2.7.2 กรณีเก็บรวบรวมข้อมูลจากแหล่งอื่น	404	8.2.7 ความสัมพันธ์ของหลักการประมวลผลข้อมูลที่น้อยที่สุดเท่าที่จำเป็น และหลักการเก็บรักษาข้อมูลอย่างจำกัด	436
7.2.8 ตัวอย่างการแจ้งรายละเอียดในรูปแบบ “นโยบายคุ้มครองข้อมูล ส่วนบุคคล” (Privacy policy)	406	8.3 หลักความถูกต้อง (Accuracy)	438
7.3 การกระทำต่อข้อมูลส่วนบุคคลเพิ่มเติมหรือแตกต่างจากวัตถุประสงค์ ที่แจ้งไว้ (Further processing of personal data)	411	8.3.1 ความถูกต้อง ประกอบด้วยคุณลักษณะด้านคุณภาพ หรือมาตรฐานหลายประการ	439
บทที่ 8 หลักกฎหมายเกี่ยวกับมาตรฐานและคุณภาพของข้อมูลส่วนบุคคล	419	8.3.2 ข้อมูลที่เป็นปัจจุบัน (Up to date)	439
8.1 หลักการประมวลผลข้อมูลที่น้อยที่สุดเท่าที่จำเป็น (Data minimization)	419	8.3.3 ข้อมูลที่ผิดพลาด (Mistake) และข้อมูลที่ทำให้เกิดความเข้าใจผิด (Misleading)	441
8.1.1 การเก็บรวบรวมข้อมูลน้อยเกินไปอาจไม่สอดคล้องกับหลักการ ประมวลผลข้อมูลที่น้อยที่สุด	421	8.3.4 ความถูกต้องของข้อมูลส่วนบุคคลที่เป็นความคิดเห็น	442
8.1.2 การเก็บรวบรวมข้อมูลเพื่อวัตถุประสงค์บางประการในอนาคต	422	8.4 โทษของการฝ่าฝืนหลักกฎหมายเกี่ยวกับมาตรฐานและคุณภาพ ของข้อมูลส่วนบุคคล	442
8.1.3 การเก็บข้อมูลเพื่อรองรับการดำเนินการในอนาคตที่ไม่เกี่ยวกับ วัตถุประสงค์ในขั้นตอนการเก็บรวบรวมข้อมูล	423		

บทที่ 9 หน้าที่การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย

ของข้อมูลส่วนบุคคล	444
9.1 ภาพรวมของหลักกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัย ของข้อมูลส่วนบุคคล	445
9.2 ภัยคุกคามความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือการละเมิด ข้อมูลส่วนบุคคล	446
9.2.1 กรอบแนวคิดเกี่ยวกับเกณฑ์จำแนกภัยคุกคามทางคอมพิวเตอร์	447
9.2.2 ภัยคุกคามความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือ การละเมิดข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	449
9.2.2.1 ภัยคุกคามข้อมูลส่วนบุคคลหรือการละเมิดข้อมูลส่วนบุคคล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR)	449
9.2.2.2 ภัยคุกคามข้อมูลส่วนบุคคลหรือการละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	450
9.2.3 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาจากผู้ก่อภัยคุกคาม	454
9.2.3.1 การจำแนกภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาความสัมพันธ์ระหว่างผู้ก่อภัยคุกคามและผู้ควบคุม ข้อมูลส่วนบุคคล	454
9.2.3.2 การจำแนกภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคลโดย พิจารณาเจตนาของผู้ก่อภัยคุกคาม	455
9.2.4 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยพิจารณาวิธีการและเป้าหมาย	457
9.2.5 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล ที่ไม่ได้เกิดจากการกระทำของบุคคล	458
9.2.6 การจำแนกประเภทภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล โดยคุณลักษณะด้านความปลอดภัยทางคอมพิวเตอร์	458
9.2.7 ภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคลกับอาชญากรรม คอมพิวเตอร์ในกรอบพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์	461

9.2.8 หน้าที่และความรับผิดชอบตามกฎหมายของผู้เกี่ยวข้องกับภัยคุกคาม หรือการละเมิดข้อมูลส่วนบุคคล	465
9.2.9 ผลกระทบจากภัยคุกคามหรือการละเมิดข้อมูลส่วนบุคคล	468
9.3 มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	472
9.3.1 รายละเอียดตามกฎหมายของมาตรการหรือมาตรฐานการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	472
9.3.1.1 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563	473
9.3.1.2 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูล ส่วนบุคคล พ.ศ. 2565	476
9.3.1.3 มาตรการหรือมาตรฐานการรักษาความมั่นคงปลอดภัยของ ข้อมูลส่วนบุคคลตาม GDPR	480
9.3.2 บุคคลที่ต้องรับผิดชอบและประเด็นเกี่ยวกับเจตนา	482
9.3.3 ปัจจัยในการพิจารณา “ความเหมาะสม” ของมาตรการรักษา ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	483
9.3.4 ปัจจัยเกี่ยวกับความเสี่ยง (Risk) ของผลกระทบหรือความเสียหาย ต่อเจ้าของข้อมูลส่วนบุคคล	485
9.3.5 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลด้านต่างๆ	486
9.4 กรณีศึกษาในทางคดีเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล	491
9.5 กรอบแนวทางการร่างนโยบายรักษาความมั่นคงปลอดภัย ของข้อมูลส่วนบุคคล	496
9.6 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal data breach notification)	505
9.6.1 ผู้มีหน้าที่แจ้งและผู้รับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล	506
9.6.2 เงื่อนไขเบื้องต้นในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	507
9.6.3 กระบวนการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	509

9.6.4 เนื้อหาและรายละเอียดของการแจ้งการละเมิดข้อมูลส่วนบุคคล	522
9.6.5 ข้อยกเว้นที่เกี่ยวข้องกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	524
บทที่ 10 หน้าที่ตามกฎหมายและความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล	528
10.1 หลักกฎหมายที่เกี่ยวข้องกับความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล	528
10.2 เงื่อนไขเบื้องต้นในการพิจารณาความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคล	533
10.3 สัญญาที่เกี่ยวข้องในความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับผู้ประมวลผลข้อมูลส่วนบุคคล	534
10.4 ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลหรือสัญญาประมวลผลข้อมูลส่วนบุคคล	536
10.4.1 แนวทางการร่างสัญญาประมวลผลข้อมูลส่วนบุคคลและเปรียบเทียบกับกฎหมายสหภาพยุโรป	537
10.4.2 ส่วนของชื่อและคู่สัญญา	539
10.4.3 อาร์มบทหรือเกริ่นนำ (Preamble)	539
10.4.4 นิยาม (Definition)	541
10.4.5 สิทธิและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	542
10.4.6 คำสั่งของผู้ควบคุมข้อมูลต่อผู้ประมวลผลและข้อกำหนดห้ามมิให้ผู้ประมวลผลทำการนอกเหนือจากคำสั่ง	543
10.4.7 ข้อสัญญาเกี่ยวกับหน้าที่รักษาความลับ (Duty of confidence)	544
10.4.8 ข้อสัญญาเกี่ยวกับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล	546
10.4.9 ข้อสัญญาเกี่ยวกับผู้ประมวลผลช่วง (Sub-processor)	548
10.4.10 ข้อสัญญากำหนดหน้าที่ผู้ประมวลผลในการช่วยเหลือผู้ควบคุมข้อมูลให้ปฏิบัติหน้าที่ตามกฎหมาย	550
10.4.11 ข้อสัญญาเกี่ยวกับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	551
10.4.12 ข้อสัญญาเกี่ยวกับการลบหรือส่งคืนข้อมูลส่วนบุคคล	552

บทที่ 11 สิทธิของเจ้าของข้อมูลส่วนบุคคล	554
11.1 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of access)	555
11.2 สิทธิในการแก้ไขข้อมูลส่วนบุคคล (Right to rectification)	564
11.3 สิทธิในการขอให้ลบข้อมูลส่วนบุคคล (Right to erasure) หรือสิทธิที่จะถูกลืม (Right to be forgotten)	565
11.3.1 สิทธิที่จะถูกลืมตามกฎหมายสหภาพยุโรปก่อน GDPR	566
11.3.2 เปรียบเทียบสิทธิที่จะถูกลืมตาม GDPR กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	568
11.3.2.1 หลักทั่วไปของสิทธิที่จะถูกลืม	568
11.3.2.2 เหตุแห่งการใช้สิทธิในการลบข้อมูลส่วนบุคคล	569
11.3.2.3 ข้อยกเว้นหรือข้อจำกัดสิทธิในการลบข้อมูลส่วนบุคคล	571
11.3.3 เปรียบเทียบคำพิพากษาศาลยุโรปกับสิทธิในการลบข้อมูลส่วนบุคคลตามกฎหมายไทย	572
11.3.4 สิทธิที่จะถูกลืม เปรียบเทียบกับการลบหรือทำลายข้อมูลตามกฎหมายอื่น	577
11.4 สิทธิในการคัดค้านการประมวลข้อมูลส่วนบุคคล (Right to object)	579
11.4.1 เงื่อนไขและข้อจำกัดสิทธิคัดค้าน	579
11.4.2 การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล	582
11.5 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing)	583
11.5.1 เงื่อนไขของการใช้สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล	583
11.5.2 การดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล	585
11.6 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to data portability)	586
11.7 สิทธิในการได้รับแจ้งข้อมูลหรือรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Right to be informed)	589
11.8 ประเด็นพิจารณาเกี่ยวกับสิทธิของเจ้าของข้อมูล	591
11.8.1 รูปแบบและวิธีการร้องขอใช้สิทธิ	591

11.8.2 การบันทึกการเกี่ยวกับสิทธิของเจ้าของข้อมูล	595
11.8.3 ค่าธรรมเนียมของการใช้สิทธิ	597
11.8.4 การสร้างเงื่อนไขของการใช้สิทธิที่เป็นอุปสรรคต่อเจ้าของข้อมูล	598
11.9 ความสัมพันธ์ระหว่างสิทธิของเจ้าของข้อมูลกับเหตุหรือฐานทางกฎหมาย	599
11.10 สิทธิเจ้าของข้อมูลบางประการที่กฎหมายไทยไม่ได้บัญญัติไว้เป็นการเฉพาะ	602
บทที่ 12 ความรับผิด โทษ และการร้องเรียน	605
12.1 ความรับผิดและโทษของผู้ควบคุมข้อมูลส่วนบุคคล	605
12.1.1 ความรับผิดทางแพ่ง	605
12.1.2 โทษอาญา	616
12.1.2.1 ความผิดมาตรา 79 วรรคหนึ่ง	617
12.1.2.2 ความผิดมาตรา 79 วรรคสอง	621
12.1.2.3 ความผิดมาตรา 81	623
12.1.2.4 กรณีศึกษา การนำฐานความผิดอาญาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้ดำเนินคดีกับข้อพิพาทในสื่อสังคมออนไลน์ของประชาชนทั่วไป	624
12.1.3 โทษปรับทางปกครอง	627
12.2 ความรับผิดและโทษของผู้ประมวลผลข้อมูลส่วนบุคคล	632
12.2.1 ความรับผิดทางแพ่ง	632
12.2.2 โทษทางอาญา	632
12.2.3 โทษปรับทางปกครอง	633
12.3 ความรับผิดและโทษสำหรับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผล	637
12.4 ความรับผิดและโทษที่ไม่จำกัดสถานะของบุคคล	638
12.4.1 โทษปรับทางปกครอง	638

12.4.2 โทษทางอาญาล่วงรู้และเปิดเผยข้อมูลส่วนบุคคล	638
12.5 การร้องเรียน	644
12.5.1 การร้องเรียนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	644
12.5.2 เปรียบเทียบการร้องเรียนตามกฎหมายสหภาพยุโรป	647

บทส่งท้าย ข้อจำกัดและผลกระทบทางลบ

ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล	651
--	-----

บรรณานุกรม	677
------------------	-----

ภาคผนวก

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	695
- พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563	741
- กฎกระทรวง กำหนดลักษณะของวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2562	745
- ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563	747
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563	750
- พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564	752
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกการเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565	755
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565	757

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูล ส่วนบุคคล พ.ศ. 2565	759
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565	763
- พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงานที่ได้รับยกเว้น ไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566	768
ดัชนีค้นคำ	768
ประวัติผู้เขียน	777