THE GOVERNMENT PUBLIC RELATIONS DEPARTMENT

แนวทางการตรวจสอบสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ASSESSMENT GUIDELINES FOR THE PERSONAL DATA PROTECTION OFFICER

โครงการจัดจ้างวิเคราะห์และจัดทำแนวทางมาตรการในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคล ตามโครงการธรรมาภิบาลข้อมูลภาครัฐ กปส.
(PRD Data Governance)

JUL 2022

PREPARED BY

THAMMASAT UNIVERSITY
RESEARCH AND CONSULTANCY INSTITUTE
สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

Document Control

Document Owner	กรมประชาสัมพันธ์
Document Preparer	สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์
Date Created	6/15/2022
Date Last Modified	7/22/2022
Document Name	แนวทางการตรวจสอบสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Assessment Guidelines for the Personal Data Protection Officer)
Version	1.0
Status	Final

Document Change Record

Version	Date Last Modified	By	Details of modification
1.0	7/22/2022	TU	Final

Document Review

Name	Position

Document Approver

Name	Position	Signature	Date
			Click or tap to enter a date.

Contents

Document Control

Document Change Record

Document Review

Document Approver

คำนิยาม ... 1

หลักการและเหตุผล ... 4

วัตถุประสงค์ ... 4

ขอบเขต ... 4

บทบาท อำนาจ และหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ... 5

แนวทางการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ... 6

1. โครงสร้างของการกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ ... 7
2. นโยบายคุ้มครองข้อมูลส่วนบุคคล ... 11
3. การจัดทำและปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ... 12
4. การเลือกฐานทางกฎหมายเพื่อการเก็บรวบรวมข้อมูลส่วนบุคคล ... 12
5. การประเมินเพื่อใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย ... 12
6. การดำเนินการเพื่อขอความยินยอม ... 13
7. การขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว ... 14
8. การขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ ... 15
9. การบริหารจัดการความยินยอม ... 16
10. การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล ... 17
11. การเก็บรวบรวมข้อมูลส่วนบุคคล ... 18
12. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ... 19
13. การใช้และเปิดเผยข้อมูลส่วนบุคคล ... 19
14. หลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ ... 20
15. การจัดส่งข้อมูลส่วนบุคคลไปยังต่างประเทศ ... 22
16. การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอก ... 23
17. การจ้างผู้ให้บริการภายนอกที่มีสัญญาหรือข้อตกลงการให้บริการ ... 24

18. การพิจารณาความเสี่ยงที่เกี่ยวข้องกับงานจ้างผู้ให้บริการภายนอกและกำหนดมาตรการที่จำเป็นลงสัญญา หรือข้อตกลงการให้บริการเพื่อให้ผู้ให้บริการภายนอกปฏิบัติตาม 24

19. การดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล 25

20. การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 25

21. การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล 27

22. การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล 28

Table Contents

ตาราง 1 คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) มีความรู้ ความเข้าใจ ตลอดจนความตระหนักในหน้าที่ และความรับผิดชอบ 7

ตาราง 2 การกำหนดหลักเกณฑ์การคัดเลือกผู้ให้บริการภายนอก 8

ตาราง 3 จัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการภายนอก 10

ตาราง 4 การตรวจสอบและประเมินนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร 11

ตาราง 5 การประเมินเพิ่มเติมสำหรับบันทึกกิจกรรมการประมวลผล 12

ตาราง 6 การดำเนินการก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล 12

ตาราง 7 การประเมินความจำเป็นของการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย 12

ตาราง 8 การดำเนินการในการขอความยินยอมก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล 13

ตาราง 9 การดำเนินการในการขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว 14

ตาราง 10 การดำเนินการในการขอความยินยอมสำหรับการขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ 15

ตาราง 11 การดำเนินการในการบริหารจัดการความยินยอม 16

ตาราง 12 การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล 18

ตาราง 13 การดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลตามหลักการสากลสำหรับการคุ้มครองข้อมูลส่วนบุคคล 18

ตาราง 14 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล 19

ตาราง 15 การดำเนินการต่าง ๆสำหรับการใช้และเปิดเผยข้อมูลส่วนบุคคล 19

ตาราง 16 หลักเกณฑ์สำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่เกี่ยวข้อง 20

ตาราง 17 การพิจารณาประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ 21

ตาราง 18 การพิจารณาการการได้รับการยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสามารถโอนย้ายข้อมูลไปยังต่างประเทศ 21

ตาราง 19 กรณีเป็นหน่วยงานในต่างประเทศที่มีอำนาจหน้าที่ที่เกี่ยวข้องร้องขอให้จัดส่ง 22

ตาราง 20 การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอกมีการดำเนินการ 23

ตาราง 21 สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก 24

ตาราง 22 สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก 25

ตาราง 23 พิจารณาตรวจสอบการแจ้งและการจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล 25

ตาราง 24 พิจารณากรณีเหตุละเมิดมีผลกระทบสูง 26

ตาราง 25 พิจารณาประเมินการจัดเก็บรักษาและระยะเวลาในการจัดเก็บ 27

ตาราง 26 การจำหน่ายออกและลบทำลายข้อมูลส่วนบุคคลขององค์กร 28

ตาราง 27 การดำเนินการจำหน่ายออกข้อมูลส่วนบุคคลขององค์กร 28

คำนิยาม

คำศัพท์	ความหมาย
องค์กร	กรมประชาสัมพันธ์ (“กปส.”)
ที่ปรึกษา	สำนักงานศูนย์วิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะเช่น ชื่อ นามสกุล ชื่อเล่น ที่อยู่ หมายเลขโทรศัพท์ เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต ที่อยู่อีเมล (email address) ทะเบียนรถยนต์ IP Address, Cookies, Log File เป็นต้น
เจ้าของข้อมูลส่วนบุคคล	บุคคลธรรมดาที่สามารถระบุตัวตนได้จากข้อมูลส่วนบุคคล และให้หมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ รวมตลอดทั้งผู้ที่ถือว่าเป็นเจ้าของข้อมูลส่วนบุคคลภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
ชอบด้วยกฎหมาย	มีความถูกต้องตามกฎหมายทุกประการ เช่น การดำเนินการขององค์กรที่ชอบด้วยกฎหมาย จึงหมายถึง การดำเนินการขององค์กรที่มีความถูกต้องตามกฎหมายทุกประการ
ฐานทางกฎหมาย	การอธิบายหรือแสดงเหตุผลที่สมเหตุสมผลและชอบด้วยกฎหมายว่าทำไมคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) จึงจำเป็นต้องเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลหนึ่ง (อ้างอิงจาก https://www.termsfeed.com/blog/gdpr-lawful-basis-processing/)
การประมวลผลข้อมูลส่วนบุคคล	การดำเนินการใดๆ กับข้อมูลส่วนบุคคล (อันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในลักษณะใดลักษณะหนึ่งได้) เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบ จัดโครงสร้าง การปรับปรุงหรือการแก้ไขข้อมูล การดึงข้อมูล การให้คำปรึกษาที่ต้องใช้ข้อมูลในการให้คำปรึกษา การใช้ข้อมูล การเปิดเผยด้วยการส่งต่อ การเผยแพร่ หรือ การกระทำใด ๆ เพื่อให้ข้อมูลสามารถเข้าถึงหรือใช้งานได้ การรวมข้อมูลเข้าด้วยกัน การดำเนินการเพื่อให้ข้อมูลสอดคล้องกัน การจำกัดการใช้งาน การลบ หรือการทำลายข้อมูล
การคุ้มครองข้อมูลส่วนบุคคล	การดูแลปกป้องบุคคลจากการถูกละเมิดเกี่ยวกับข้อมูลส่วนบุคคลโดยกฎหมาย ซึ่งเป็นการจำกัดสิทธิและเสรีภาพบางประการของบุคคลที่เก็บรวบ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น เพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคล และมาตรการเยียวยาเจ้าของข้อมูลที่มีประสิทธิภาพ

คำศัพท์	ความหมาย
บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	รายการข้อมูลสำหรับใช้เป็นเครื่องมือในการควบคุมกิจกรรมการประมวลผลของข้อมูลส่วนบุคคลที่ได้มีการรวบรวม เพื่อให้การดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลนั้นเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด ลดความเสี่ยงต่างๆ ที่เกี่ยวข้อง สอดคล้องกับหลักการการคุ้มครองข้อมูลส่วนบุคคล สอดคล้องกับวิธีปฏิบัติสากล และยังทำให้มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมต่อข้อมูลส่วนบุคคลนั้น (มาตรา 39 ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้มีการจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนี้)
ความยินยอม	การแสดงเจตนาของเจ้าของข้อมูลส่วนบุคคล หรือผู้มีอำนาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคล อนุญาตให้ผู้อื่นเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล ผ่านเอกสารหรือผ่านระบบอิเล็กทรอนิกส์ โดยการกระทำข้างต้น (เก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล) จะถือว่าไม่เป็นการละเมิด ไม่ถือว่าเป็นความเสียหาย บุคคลจึงไม่มีสิทธิเรียกค่าเสียหายอันเกิดจากการกระทำที่ตนให้ความยินยอม
ทะเบียนความยินยอม	ข้อมูลการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล ที่โดยทั่วไปจะต้องมีการลงนามอนุญาตให้ใช้ข้อมูลส่วนบุคคล มีรายละเอียดข้อมูลส่วนบุคคลที่เกี่ยวข้อง ชื่อผู้ที่ให้ความยินยอม วันเวลาที่ให้การยินยอม กรณีที่มีการยกเลิกหรือถอนความยินยอม ชื่อผู้ที่ถอนความยินยอม วันเวลาที่ยกเลิกหรือถอนความยินยอม สถานะของการดำเนินการลบข้อมูลส่วนบุคคล (สำหรับกรณีที่มีการถอด ความยินยอม) ทะเบียนความยินยอมนี้อาจจะจัดทำเป็นไฟล์อิเล็กทรอนิกส์ในรูป Excel หรืออาจจะจัดทำเป็นระบบงานสารสนเทศก็ได้ จุดประสงค์สำคัญของทะเบียนความยินยอม คือ เพื่อป้องกันการใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต และเพื่อป้องกันไม่ให้องค์กรยังมีการใช้ข้อมูลส่วนบุคคลอยู่ภายหลังจากที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมไปแล้ว
ข้อมูลที่มีความอ่อนไหว	ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ ความคิดเห็นทางการเมือง ความเชื่อ ในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
การลบทำลาย	การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้อีกต่อไป โดยใครก็ตามและไม่ว่าจะที่เวลาใดก็ตาม การลบทำลายเป็นวิธีการที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพราะทำให้ไม่สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลได้อีกต่อไป

คำศัพท์	ความหมาย
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	ผู้อำนวยการฝ่ายของ สทป. ที่มีหน้าที่ให้คำแนะนำเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแก่บุคคลในองค์กร ตรวจสอบการดำเนินงานว่าสอดคล้องกับพระราชบัญญัติฯ หรือไม่ และประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
การถอนความยินยอม	สิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการถอนความยินยอมที่ให้ไว้สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยจะต้องสามารถถอนความยินยอมเมื่อใดก็ได้และสามารถทำได้โดยง่าย เว้นแต่จะมีข้อจำกัดด้านกฎหมายหรือสัญญาที่เป็นประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล โดยผู้รับคำร้องต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอม (ถ้ามี)

หลักการและเหตุผล

เนื่องจากในปัจจุบันมีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีชื่อว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act: PDPA) ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคลของประชาชน ทุกคน จากการถูกนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาติจากเจ้าของข้อมูล โดยผู้ที่จะต้องปฏิบัติตามประกอบไปด้วยหน่วยงานต่าง ๆ ทั้งภาครัฐ และภาคเอกชน ซึ่งทางกรมประชาสัมพันธ์ เป็นหน่วยงานที่อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติดังกล่าวเช่นกัน จึงต้องมีการดำเนินการบูรณาการกระบวนการดำเนินงานขององค์กรเพื่อให้สอดคล้อง และเป็นไปตามความต้องการของกฎหมาย ระเบียบ ข้อบังคับดังกล่าว

โดยหนึ่งในความต้องการของพระราชบัญญัตินี้คือ ต้องมีการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กร ดังนั้น เอกสารเล่มนี้จึงจะกล่าวถึงบทบาท อำนาจ หน้าที่ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และแนวทางการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมตามกฎหมาย

วัตถุประสงค์

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็นแนวทางการตรวจสอบสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ยึดหลักแนวทางการตรวจสอบตามเอกสารฉบับนี้ เพื่อให้การดำเนินงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และเป็นไปในแนวทางเดียวกัน

ขอบเขต

เอกสารฉบับนี้ครอบคลุมถึงแนวทางการตรวจสอบสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบด้วย บทบาท อำนาจ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และแนวทางการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยแนวทางนี้จะใช้เป็นเอกสารอ้างอิงหลักในการตรวจสอบกระบวนการดำเนินการ 22 รายการ ตามที่ระบุในเอกสารฉบับนี้

บทบาท อำนาจ และหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

หน้าที่ความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ที่ได้รับมอบหมายต้องไม่มีความขัดแย้งกับหน้าที่ความรับผิดชอบปัจจุบัน ได้มีการกล่าวไว้ใน GDPR ว่าในอำนาจหน้าที่ที่มีอยู่ในปัจจุบันนั้นจะต้องไม่มีส่วนในการกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ซึ่งจะเป็นหน้าที่ของคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) มีดังต่อไปนี้

1. ให้คำแนะนำในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล และทบทวนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
2. ติดตามผลการประเมินความเสี่ยงหรือผลการประเมินผลกระทบต่อข้อมูลส่วนบุคคลจากหน่วยงานต่าง ๆ เพื่อพิจารณาให้ข้อคิดเห็นตามความจำเป็น
3. กำหนดแนวทางการรับมือต่อเหตุละเมิดข้อมูลส่วนบุคคล และแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
4. กำหนดแนวทางการจัดการคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
5. ให้คำแนะนำและคำปรึกษารวมถึงสร้างความตระหนักเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แก่หน่วยงานต่าง ๆ
6. ตรวจสอบและทบทวนการดำเนินงานการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานต่าง ๆ ให้มีความสอดคล้อง ตามวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคลที่กำหนดไว้ และไม่ละเมิดกฎหมายระเบียบข้อบังคับ
7. ติดตามการเปลี่ยนแปลงด้านกฎหมาย มาตรการ กฎระเบียบต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
8. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามความจำเป็น
9. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่
10. รายงานไปยังคณะกรรมการติดตามผลการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล และอธิการบดีกรมประชาสัมพันธ์ในกรณีที่เกิดปัญหาในการปฏิบัติหน้าที่
11. ปฏิบัติหน้าที่อื่นใดตามที่อธิบดีกรมประชาสัมพันธ์มอบหมาย
12. ให้ฝ่าย/ส่วนงานภายในกรมประชาสัมพันธ์ ให้การสนับสนุนการปฏิบัติงานของคณะทำงานคุ้มครองข้อมูลส่วนบุคคล (DPO) ตามที่ได้รับการร้องขอ

แนวทางการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีแนวทางการตรวจสอบ 22 หัวข้อ ดังนี้

1. โครงสร้างของการกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ
2. นโยบายคุ้มครองข้อมูลส่วนบุคคล
3. การจัดทำและปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
4. การเลือกฐานทางกฎหมายเพื่อการเก็บรวบรวมข้อมูลส่วนบุคคล
5. การประเมินเพื่อใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย
6. การดำเนินการเพื่อขอความยินยอม
7. การขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว
8. การขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ
9. การบริหารจัดการความยินยอม
10. การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล
11. การเก็บรวบรวมข้อมูลส่วนบุคคล
12. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
13. การใช้และเปิดเผยข้อมูลส่วนบุคคล
14. หลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ
15. การจัดส่งข้อมูลส่วนบุคคลไปยังต่างประเทศ
16. การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอก
17. การจ้างผู้ให้บริการภายนอกที่มีสัญญาหรือข้อตกลงการให้บริการ
18. การพิจารณาความเสี่ยงที่เกี่ยวข้องกับงานจ้างผู้ให้บริการภายนอกและกำหนดมาตรการที่จำเป็นลงสัญญา หรือข้อตกลงการให้บริการเพื่อให้ผู้ให้บริการภายนอกปฏิบัติตาม
19. การดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
20. การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
21. การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล
22. การจำหน่ายออกและลบทำลายข้อมูลส่วนบุคคล

1. โครงสร้างของการกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ

คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) มีความรู้ ความเข้าใจ ตลอดจนความตระหนักในหน้าที่และความรับผิดชอบ ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบ มีความรู้และความเข้าใจในนโยบายและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยขององค์กรหรือไม่	
2.	มีความตระหนักในการปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรหรือไม่	
3.	มีความตระหนักในการให้ข้อมูลส่วนบุคคลแก่ผู้อื่นด้วยความระมัดระวังรอบคอบและป้องกันมิให้มีการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่	
4.	มีความรู้และความเข้าใจในเรื่องของการแจ้งเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่	
5.	มีความรู้และความเข้าใจ ในเรื่องของการขอความยินยอม ก่อนการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่	
6.	มีความเข้าใจในสิทธิตามกฎหมาย คุ้มครองข้อมูลส่วนบุคคล ของเจ้าของข้อมูลส่วนบุคคลหรือไม่	
7.	มีการกำหนดขั้นตอนปฏิบัติสำหรับการรับเรื่องการขอใช้สิทธิโดยเจ้าของข้อมูลส่วนบุคคลหรือไม่	
8.	กรณีที่มีการปฏิเสธการร้องขอใช้สิทธิ มีการบันทึกเหตุผลของการปฏิเสธไว้หรือไม่	
9.	ได้กำหนดให้มีวิธีการอย่างเป็นรูปธรรมสำหรับ การตรวจสอบและทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาจัดเก็บหรือไม่	
10.	มีการดูแลคุณภาพของข้อมูลให้มีความถูกต้องและความครบถ้วนตลอดระยะเวลาการ ใช้งานข้อมูลของตนเองหรือไม่	
11.	มีการประเมินความเสี่ยงหรือประเมินผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลหรือไม่ มีแผนการจัดการกับความเสี่ยงอย่างเป็นรูปธรรมหรือไม่	
12.	มีการทำบันทึกกิจกรรมการประมวลผลของข้อมูลส่วนบุคคลที่ตนเองต้องรับผิดชอบหรือไม่	

ตาราง 1 คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) มีความรู้ ความเข้าใจ ตลอดจนความตระหนักในหน้าที่ และความรับผิดชอบ

มีการกำหนดหลักเกณฑ์การคัดเลือกผู้ให้บริการภายนอก ในลักษณะดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	งานที่จ้างให้ทำไม่ซับซ้อนและจำนวนข้อมูลส่วนบุคคลที่เปิดเผยไม่มาก	
2.	มีนโยบายคุ้มครองข้อมูลส่วนบุคคลประกาศและบังคับใช้ภายในหน่วยงาน	
3.	มีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและบังคับใช้ภายในหน่วยงาน	
4.	มีมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ดี เช่น มีการปฏิบัติตามมาตรฐาน ISO/IEC 27001	
5.	มีการจัดการกับข้อมูลตามชั้นความลับ	
6.	เคยใช้บริการจากผู้ให้บริการภายนอกรายนี้มาก่อน	
7.	มีบุคคลหรือหน่วยงานอ้างอิงที่สามารถสอบถามข้อมูลได้ ทั้งนี้เพื่อให้เกิดความมั่นใจก่อนการจ้าง	
8.	เป็นหน่วยงานภาครัฐ	
9.	เป็นหน่วยงานเอกชนที่มีความน่าเชื่อถือและเปิดให้บริการมาเป็นระยะเวลาหนึ่ง	

ตาราง 2 การกำหนดหลักเกณฑ์การคัดเลือกผู้ให้บริการภายนอก

การจัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการภายนอก มีการกำหนดหรือระบุประเด็นดังต่อไปนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด รวมทั้งการควบคุมบุคลากรหรือลูกจ้างของผู้ให้บริการภายนอกให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	
2.	กำหนดวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลลงในสัญญาหรือข้อตกลงการจ้างงานให้ชัดเจน พร้อมทั้งกำหนดให้ปฏิบัติตามวัตถุประสงค์การประมวลผลที่กำหนดไว้อย่างเคร่งครัด	
3.	กำหนดให้ผู้ให้บริการภายนอกมีการกำหนดมาตรการความมั่นคงปลอดภัย เพื่อป้องกันและรักษาข้อมูลที่องค์กรได้ให้ไว้	
4.	กำหนดให้ผู้ให้บริการภายนอกดำเนินการลบทำลายข้อมูลส่วนบุคคลที่องค์กรได้ให้ไว้ เมื่อพ้นระยะเวลาการจัดเก็บ หรือตามคำสั่งที่ได้รับจากองค์กร	
5.	กำหนดให้ผู้ให้บริการภายนอกมีการจำกัดและควบคุมการเข้าถึงข้อมูลส่วนบุคคลที่องค์กรได้ให้ไว้ เพื่อให้มีเฉพาะบุคลากรหรือลูกจ้างของผู้ให้บริการภายนอกที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้	

การจัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการภายนอก มีการกำหนดหรือระบุประเด็นดังต่อไปนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
6.	กำหนดให้ผู้ให้บริการภายนอกระมัดระวังและเคร่งครัด การปฏิบัติตามคำสั่งจากคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) สัญญาหรือข้อตกลงที่กำหนดไว้ และห้ามปฏิบัตินอกเหนือจากที่สั่งหรือที่กำหนดไว้	
7.	กำหนดห้ามผู้ให้บริการภายนอกดำเนินการจ้างช่วงไปยังหน่วยงานภายนอกอื่นใด เว้นเสียแต่ได้รับอนุมัติจากองค์กรก่อนเท่านั้น	
8.	กรณีที่ได้มีการอนุมัติการจ้างช่วงแล้ว หากผู้ให้บริการภายนอกมีการเปลี่ยนแปลงที่เกี่ยวข้องกับการรับจ้างช่วงนั้น ต้องขออนุมัติการเปลี่ยนแปลงนั้นจากองค์กรก่อนเท่านั้น องค์กรมีสิทธิปฏิเสธไม่อนุญาตการเปลี่ยนแปลงที่ขออนุมัตินั้นได้	
9.	กำหนดห้ามนำข้อมูลส่วนบุคคลที่ให้แก่ผู้ให้บริการภายนอกไปใช้ในวัตถุประสงค์ด้านการตลาดและโฆษณาประชาสัมพันธ์โดยเด็ดขาด ลงในสัญญาหรือข้อตกลงการจ้างงาน	
10.	กำหนดให้ผู้ให้บริการภายนอกประเมินความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่ได้รับจากองค์กร และเสนอแผนการจัดการกับความเสี่ยง	
11.	กำหนดให้ผู้ให้บริการภายนอกจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามรูปแบบที่องค์กรกำหนด ทบทวนและปรับปรุงบันทึกให้ทันสมัยอยู่เสมอ และส่งมอบให้องค์กรจัดเก็บไว้	
12.	กำหนดให้ผู้ให้บริการภายนอกแจ้งการเปลี่ยนแปลงที่เกี่ยวข้องกับองค์กรของตนเอง ระบบ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกอันจะกระทบกับการจ้างงานให้คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) ได้รับทราบ (เพื่อวางแผนบริหารจัดการกับการเปลี่ยนแปลงที่กำลังจะเกิดขึ้นนั้น)	
13.	ระบุลงในสัญญาหรือข้อตกลงการจ้างงานว่ากรณีเจ้าของข้อมูลส่วนบุคคล ร้องขอใช้สิทธิดำเนินการต่าง ๆ กับข้อมูลของตนเอง ผู้ให้บริการภายนอกต้องแจ้งให้องค์กรได้รับทราบก่อน เพื่อเป็นผู้อนุมัติหรือไม่อนุมัติการดำเนินการ (ยกเว้นสัญญาหรือข้อตกลงอนุญาตให้ดำเนินการได้เลย)	
14.	ระบุลงในสัญญาหรือข้อตกลงการจ้างงานว่าเมื่อมีการร้องขอหรือมีคำสั่งให้ส่งข้อมูลส่วนบุคคลจากหน่วยงานภายนอก ส่งมาที่ผู้ให้บริการภายนอก โดยหน่วยงานภายนอกเหล่านั้นอาจเป็นหน่วยงานราชการ หน่วยงานอิสระที่มีอำนาจตามกฎหมาย หรือเป็นประกาศที่มีผลบังคับทางกฎหมายให้ดำเนินการให้ผู้ให้บริการภายนอกดำเนินการแจ้งให้คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ)ได้รับทราบก่อน และห้ามผู้ให้บริการภายนอกดำเนินการโดยพลการเองโดยเด็ดขาด	

การจัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการภายนอก มีการกำหนดหรือระบุประเด็นดังต่อไปนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
15.	กำหนดให้ผู้ให้บริการภายนอกแจ้งเหตุการณ์ละเมิดความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลที่องค์กรได้ให้ไว้ภายในระยะเวลาไม่เกิน 48 ชั่วโมงนับตั้งแต่พบเหตุให้ได้รับทราบ	
16.	กำหนดให้ผู้ให้บริการภายนอกต้องไม่แจ้งเหตุละเมิดความมั่นคงปลอดภัยต่อหน่วยงานหรือผู้อื่นโดยเด็ดขาด	
17.	กำหนดให้ผู้ให้บริการภายนอกปฏิบัติตามแนวปฏิบัติสำหรับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรเฉพาะในส่วนที่เกี่ยวข้อง โดยกำหนดลงในสัญญาหรือข้อตกลงการจ้างงาน	
18.	ระบุลงในสัญญาหรือข้อตกลงการจ้างงานว่าองค์กรขอสงวนสิทธิในการตรวจติดตามการปฏิบัติงานของผู้ให้บริการภายนอก เพื่อให้ปฏิบัติตามข้อกำหนดและเงื่อนไขที่ระบุไว้ในสัญญาจ้าง กรณีพบความไม่สอดคล้อง จะขอให้ผู้ให้บริการภายนอกดำเนินการแก้ไขและแจ้งผลการแก้ไขให้ได้รับทราบด้วย	

ตาราง 3 จัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการภายนอก

2. นโยบายคุ้มครองข้อมูลส่วนบุคคล

ตรวจสอบและประเมินนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร ว่ามีประเด็นดังต่อไปนี้ครบถ้วนหรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล	
2.	การแจ้งก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล	
3.	การขอความยินยอมก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล	
4.	วิธีการหรือแหล่งในการเก็บรวบรวมข้อมูลส่วนบุคคล	
5.	ชนิดหรือประเภทของข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม	
6.	การควบคุมคุณภาพของข้อมูลส่วนบุคคลที่จัดเก็บไว้	
7.	บุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลเปิดเผยได้	
8.	การกำหนดมาตรการการรักษาความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลที่จัดเก็บไว้	
9.	การตรวจสอบเพื่อทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการจัดเก็บ	
10.	การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลภายในระยะเวลา ตามที่กฎหมายกำหนด	
11.	การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	
12.	การจัดส่งข้อมูลส่วนบุคคลไปยังต่างประเทศ	
13.	การให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลที่สามารถดำเนินการต่าง ๆ ได้อาทิ การคัดค้านการเก็บรวบรวมข้อมูลส่วนบุคคล การขอเข้าถึงข้อมูลส่วนบุคคล การขอให้โอนย้ายข้อมูล ส่วนบุคคลการขอให้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคล เจ้าของข้อมูลได้	
14.	การใช้หรือเปิดเผยข้อมูลส่วนบุคคล	
15.	การให้ข้อมูลสำหรับการติดต่อกับคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) สถานที่ติดต่อ และวิธีการติดต่อ ให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ	
16.	การให้ข้อมูลสำหรับการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ	

ตาราง 4 การตรวจสอบและประเมินนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร

3. การจัดทำและปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ประเมินเพิ่มเติมสำหรับบันทึกกิจกรรมการประมวลผลคือข้อ 5-8 แนวทางการตรวจสอบเป็น ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	ใช้แบบฟอร์มบันทึกกิจกรรมการประมวลผลตามที่กำหนดหรือไม่	
2.	ขึ้นทะเบียนกิจกรรมการประมวลผลครบถ้วนหรือไม่	
3.	กรอกข้อมูลครบถ้วน ถูกต้องหรือไม่	
4.	มีการทบทวนและปรับปรุงบันทึกกิจกรรมการประมวลผล อย่างสม่ำเสมอหรือไม่	

ตาราง 5 การประเมินเพิ่มเติมสำหรับบันทึกกิจกรรมการประมวลผล

4. การเลือกฐานทางกฎหมายเพื่อการเก็บรวบรวมข้อมูลส่วนบุคคล

ก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล มีการดำเนินการ ดังนี้หรือไม่

ก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล มีการดำเนินการ ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	มีการกำหนดฐานการประมวลผลหรือฐานทางกฎหมายของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมหรือไม่	

ตาราง 6 การดำเนินการก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล

5. การประเมินเพื่อใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย

ภายใต้กิจกรรมการประมวลผลข้อมูลส่วนบุคคลหนึ่ง ในการตัดสินใจประมวลผลข้อมูลส่วนบุคคลนั้นโดยใช้ฐานประโยชน์ โดยชอบด้วยกฎหมาย (Legitimate Interest) ตรวจสอบการดำเนินการดังนี้

การประเมินความจำเป็นของการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	ใช้แบบฟอร์มการประเมินความจำเป็นของการใช้ฐานประโยชน์โดยชอบด้วยกฎหมายที่กำหนดหรือไม่	
2.	นำกิจกรรมที่เป็นฐาน legitimate มาประเมินครบถ้วนหรือไม่	
3.	กรอกข้อมูลครบถ้วน ถูกต้องหรือไม่	
4.	มีการทบทวนหรือตรวจสอบอย่างสม่ำเสมอ สำหรับประเภทของข้อมูลส่วนบุคคลที่องค์กรได้มีการจัดเก็บไว้และใช้ฐานการประมวลผลประโยชน์โดยชอบด้วยกฎหมายนี้ มีความเหมาะสมหรือไม่ ที่ต้องใช้ฐานการประมวลผลนี้	

ตาราง 7 การประเมินความจำเป็นของการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย

6. การดำเนินการเพื่อขอความยินยอม

มีการดำเนินการดังต่อไปนี้หรือไม่ ในการขอความยินยอมก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล

มีการดำเนินการในการขอความยินยอมก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	ดำเนินการขอความยินยอมโดยปฏิบัติตามหลักการการคุ้มครองข้อมูลส่วนบุคคลสากลที่กำหนดไว้ เช่น การขอความยินยอมต้องเป็นไปด้วยความโปร่งใส สอดคล้องกับกฎหมาย เป็นไปด้วยความยุติธรรม เป็นต้น หรือไม่	
2.	เมื่อวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลมี การเปลี่ยนแปลงไปจากเดิม เช่น เป็นวัตถุประสงค์ไม่หรือเป็นวัตถุประสงค์เพิ่มเติม หรือเป็นวัตถุประสงค์ที่มีความเฉพาะเจาะจง ที่ยังไม่เคยนำมาปฏิบัติกับเจ้าของข้อมูลส่วนบุคคลมาก่อน มีการขอความยินยอมจากเจ้าของข้อมูลใหม่หรือไม่	
3.	การขอความยินยอมมีการดำเนินการในรูปแบบใด โดยทำเป็นหนังสือขอความยินยอม ทำผ่านระบบอิเล็กทรอนิกส์ หรือใช้เป็นระบบเสียงเพื่อขอความยินยอม เช่น โดยผ่านทางระบบ Interactive Voice Response (IVR) ของ Call Center เป็นต้น	
4.	ข้อความหรือภาษาที่ใช้ในการขอความยินยอมมีความชัดเจนหรือไม่ คลุมเครือหรือไม่ ข้อความมีลักษณะเป็นการหลอกลวงหรือทำให้เข้าใจผิดได้หรือไม่	
5.	การขอความยินยอมมีการให้สิทธิทุกประการแก่เจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้หรือไม่ อาทิ การคัดค้านการเก็บรวบรวมข้อมูลส่วนบุคคล การขอเข้าถึงข้อมูลส่วนบุคคล การขอให้โอนย้ายข้อมูลส่วนบุคคล การขอให้ดำเนินการลบ/ทำลาย หรือให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลได้	
6.	การขอความยินยอมให้ความเป็นอิสระแก่เจ้าของข้อมูลส่วนบุคคลที่จะให้หรือไม่ให้ความยินยอมก็ได้หรือไม่ การขอความยินยอมแยกส่วนออกจากข้อความอื่นอย่างชัดเจนหรือไม่ โดยไม่นำไปรวมอยู่กับเงื่อนไขการให้บริการ (Terms & Conditions) หรือข้อความในสัญญา อันจะก่อให้เกิดความสับสนแก่เจ้าของข้อมูลส่วนบุคคลได้	
7.	มีการจัดทำเป็นทะเบียนเพื่อใช้ในการควบคุมการให้ความยินยอมและการขอถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือไม่ และมีการดำเนินการปรับปรุงทะเบียนนี้ให้เป็นปัจจุบันอยู่เสมอหรือไม่	
8.	มีการจัดช่องทางโดยสะดวกเพื่อถอนความยินยอม และต้องกระทำได้โดยง่ายในระดับเดียวกับการให้ความยินยอม หรือไม่	

ตาราง 8 การดำเนินการในการขอความยินยอมก่อนหรือในระหว่างที่เก็บรวบรวมข้อมูลส่วนบุคคล

7. การขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว

มีการดำเนินการในการขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	องค์กรมีการจัดเก็บข้อมูลที่มีความอ่อนไหวตามที่กฎหมายกำหนด ดังต่อไปนี้หรือไม่ • ข้อมูลความเชื่อในลัทธิ ศาสนาหรือปรัชญา เชื้อชาติ ประวัติสุขภาพหรือการรักษาพยาบาล ประวัติอาชญากรรม ข้อมูลชีวภาพ • ข้อมูลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศและกำหนดเพิ่มเติม	
2.	องค์กรได้ทบทวนว่ายังมีความจำเป็นต้องจัดเก็บข้อมูลอ่อนไหวดังกล่าวหรือไม่ กรณีที่พบว่าไม่มีความจำเป็นแล้ว มีการยกเลิก การจำหน่ายออก และการลบทำลายข้อมูลส่วนบุคคลดังกล่าวทิ้งไปหรือไม่	
3.	คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) และบุคลากรขององค์กรมีความรู้ ความเข้าใจ และ ความตระหนักต่อข้อมูลที่มีความอ่อนไหวที่จัดเก็บไว้หรือไม่ มีการป้องกันข้อมูลเหล่านั้นอย่างเพียงพอหรือไม่	
4.	มีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยเป็นพิเศษหรือเพิ่มเติมสำหรับข้อมูลที่มีความอ่อนไหวหรือไม่	

ตาราง 9 การดำเนินการในการขอความยินยอมสำหรับการใช้ข้อมูลที่มีความอ่อนไหว

8. การขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ

<table>
<tr><th colspan="3">มีการดำเนินการในการขอความยินยอมสำหรับการขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถดังนี้หรือไม่</th></tr>
<tr><th colspan="2">หัวข้อ</th><th>ผลการตรวจสอบ/หลักฐาน</th></tr>
<tr><td>1.</td><td>คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) และบุคลากรขององค์กร มีความรู้และความเข้าใจ เกี่ยวกับประเภทของ บุคคลดังนี้หรือไม่ผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ และมีการขอความยินยอมก่อน การใช้ข้อมูลของ บุคคลเหล่านี้หรือไม่</td><td></td></tr>
<tr><td>2.</td><td>ในแต่ละประเภทของบุคคลดังกล่าว การขอความยินยอม ได้ดำเนินการดังนี้หรือไม่
• กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะ (หมายถึง ผู้มีอายุไม่ครบ 20 ปีบริบูรณ์ หรือ ไม่ได้จดทะเบียนสมรสกนก่อนอายุ 20 ปีโดยอายุไม่ต่ำกว่า 17 ปี) การให้ความยินยอมของผู้เยาว์ ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมได้โดยลำพังตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือ มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์
• กรณีเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ที่มีอายุไม่เกินสิบปี คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์
• กรณีเจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ หรือเป็นคนเสมือนไร้ความสามารถ (เช่น ผู้ป่วยทางจิต หรือผู้ที่ไม่สามารถช่วยเหลือตนเองได้ หรือผู้ป่วยที่มีอาการทางสมองหรือสมองตาย เป็นต้น) คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ)ต้องได้รับความยินยอมจากผู้อนุบาล หรือผู้พิทักษ์ที่มีอำนาจกระทำ การแทนคนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถนั้น</td><td></td></tr>
</table>

ตาราง 10 การดำเนินการในการขอความยินยอมสำหรับการขอความยินยอมสำหรับการใช้ข้อมูลส่วนบุคคลของผู้เยาว์ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ

9. การบริหารจัดการความยินยอม

มีการดำเนินการในการบริหารจัดการความยินยอม ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	มีการจัดทำทะเบียนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและปรับปรุงทะเบียนข้อมูลให้เป็นปัจจุบันอยู่เสมอ หรือไม่	
2.	เมื่อได้มีการขอความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว และเจ้าของข้อมูลส่วนบุคคลอนุญาตให้ใช้ข้อมูลที่เก็บรวบรวมนั้นได้ มีการบันทึกรายละเอียดและสถานะของ การให้ความยินยอมลงในทะเบียนความยินยอม หรือไม่	
3.	เมื่อได้รับคำร้องขอใช้สิทธิถอนความยินยอมในการใช้งานข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล และเมื่อตรวจสอบดูแล้ว ไม่มีข้อขัดแย้ง ไม่มีผลกระทบใด หรือคำปฏิเสธใด ที่องค์กรจะไม่สามารถดำเนินการให้ได้ มีการดำเนินการดังนี้ หรือไม่ • มีการดำเนินการถอนความยินยอมให้ตามความประสงค์ของเจ้าของข้อมูลส่วนบุคคลหรือไม่ • มีการบันทึกข้อมูลการถอนความยินยอมนั้นลงในทะเบียนความยินยอม หรือไม่ • มีการแจ้งระยะเวลาดำเนินการลบข้อมูลส่วนบุคคลและดำเนินการอื่นๆ ที่จำเป็นให้เสร็จสิ้นภายในระยะเวลาที่สมเหตุสมผลให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ หรือไม่ • เมื่อดำเนินการลบข้อมูลส่วนบุคคลและดำเนินการอื่นๆ ที่จำเป็นเป็นที่เรียบร้อยแล้ว มีการแจ้งให้เจ้าของข้อมูลได้รับทราบเพื่อปิดงานถอนความยินยอม หรือไม่	

ตาราง 11 การดำเนินการในการบริหารจัดการความยินยอม

10. การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล

มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	มีการกำหนดหัวข้อตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ดังนี้หรือไม่ (ในเอกสารแจ้งเก็บรวบรวมข้อมูลส่วนบุคคล) 1. วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย 2. แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา 3. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ 4. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย 5. ข้อมูลเกี่ยวกับคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย 6. สิทธิของเจ้าของข้อมูลส่วนบุคคล	
2.	มีการระบุข้อมูลแต่ละประเภทที่จะมีการเก็บรวบรวมอย่างชัดเจนหรือไม่	
3.	มีการระบุวัตถุประสงค์ของการเก็บรวบรวมอย่างชัดเจนหรือไม่ ข้อมูลแต่ละประเภทและวัตถุประสงค์เชื่อมโยงกันหรือไม่	
4.	ข้อมูลแต่ละประเภทมีการกล่าวถึงแหล่งในการเก็บรวบรวมข้อมูล เวลาที่เก็บหรือสถานที่ที่ทำการเก็บรวบรวมข้อมูลหรือไม่	
5.	ข้อมูลแต่ละประเภทมีการระบุไว้หรือไม่ว่าอยู่ในฐานการประมวลผล หรือฐานทางกฎหมายใด	
6.	ข้อมูลแต่ละประเภทมีการระบุระยะเวลาการจัดเก็บไว้อย่างชัดเจนหรือไม่ และอธิบายเหตุผล ประกอบไว้ด้วยหรือไม่ ว่าทำไมจึงต้องจัดเก็บไว้ตามระยะเวลาดังกล่าว	
7.	ข้อมูลแต่ละประเภทสามารถระบุแหล่งที่มาของการเก็บรวบรวมอย่างชัดเจนหรือไม่	
8.	ข้อมูลแต่ละประเภทมีการแจ้งให้ทราบเกี่ยวกับการเปิดเผยข้อมูลให้แก่บุคคลหรือหน่วยงานอื่นหรือไม่ และแจ้งให้ใครหรือหน่วยงานใดบ้าง ข้อมูลแต่ละประเภทมีใครเป็นคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) มีการกำหนดสถานที่ติดต่อ และวิธีการติดต่อไว้หรือไม่ รวมทั้งมีใครเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อมีการกำหนดไว้หรือไม่	

มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
9.	มีการกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลที่สามารถดำเนินการต่าง ๆ กับข้อมูลของตนเอง ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้หรือไม่	
10.	กรณีมีการส่งข้อมูลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ มีการกล่าวถึงเขตอำนาจศาลของกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งของราชอาณาจักรไทยและของประเทศอื่น ๆ หรือไม่	
11.	มีการกล่าวถึงการปรับปรุงเอกสารแจ้งเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ มีการระบุการจัดเก็บเป็นเวอร์ชั่นไว้หรือไม่ และสามารถตรวจสอบเอกสารนั้นได้จากที่ใด	

ตาราง 12 การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคล

11. การเก็บรวบรวมข้อมูลส่วนบุคคล

การดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลตามหลักการสากลสำหรับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	คณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) และบุคลากรขององค์กรปฏิบัติตามหลักการสากลสำหรับการคุ้มครองข้อมูลส่วนบุคคลดังนี้หรือไม่ ในการเก็บรวบรวมข้อมูลส่วนบุคคล (ดูรายละเอียดของแต่ละหลักการในหัวข้อหลักการการคุ้มครองข้อมูลส่วนบุคคล) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย • ความโปร่งใส (Transparency) ความสอดคล้องกับฐานทางกฎหมาย (Lawfulness) ความยุติธรรม (Fairness) • การจำกัดวัตถุประสงค์ (Purpose Limitation) • การจำกัดข้อมูลให้น้อยที่สุด (Data Minimisation) • ความถูกต้อง (Accuracy) • การจำกัดการจัดเก็บข้อมูล (บนสื่อบันทึกข้อมูล) (Storage Limitation) • ความถูกต้อง ความลับ และ ความพร้อมใช้ของข้อมูล (Information Security: Integrity, Confidentiality and Availability) • ความรับผิดชอบ (Accountability) • มีการเก็บข้อมูลอื่นใดที่นอกเหนือจากวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่	

ตาราง 13 การดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลตามหลักการสากลสำหรับการคุ้มครองข้อมูลส่วนบุคคล

12. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	ใช้แบบฟอร์มการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดหรือไม่	
2.	นำกิจกรรมที่ขึ้นทะเบียนมาประเมินครบถ้วนหรือไม่	
3.	ผลการประเมินเหมาะสมหรือไม่	
4.	มีการทบทวนหรือตรวจสอบผลการประเมินอย่างสม่ำเสมอหรือไม่	

ตาราง 14 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

13. การใช้และเปิดเผยข้อมูลส่วนบุคคล

มีการดำเนินการต่าง ๆสำหรับการใช้และเปิดเผยข้อมูลส่วนบุคคล ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	มีการใช้งานข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กำหนดไว้เท่านั้น หรือไม่	
2.	การเปิดเผยเป็นไปตามตามวัตถุประสงค์ของการประมวลผลที่กำหนดไว้ วัตถุประสงค์ที่กำหนดไว้ในสัญญาหรือข้อตกลง ตามที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือวัตถุประสงค์ตามที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลในขณะเก็บรวบรวมข้อมูลส่วนบุคคล	
3.	การเปิดเผยเพื่อให้เป็นไปตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ	
4.	นอกเหนือจากจากการเปิดเผยตามเงื่อนไขดังกล่าวนั้น มีการเปิดเผยข้อมูลส่วนบุคคลไปยังผู้อื่นหรือหน่วยงานอื่นอีก หรือไม่	
5.	มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคลให้สามารถเข้าถึงได้เฉพาะ ผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลนั้นเท่านั้น หรือไม่	
6.	มีการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรเพื่อให้ข้อมูลส่วนบุคคลที่จัดเก็บไว้มี ความมั่นคงปลอดภัยอยู่เสมอ หรือไม่	
7.	เมื่อมีการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้บุคคลหรือหน่วยงานภายนอกที่มีอำนาจหน้าที่ตามกฎหมาย มีการจัดทำ บันทึกการส่งหรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลหรือหน่วยงานภายนอกนั้น หรือไม่ เพื่อใช้เป็นหลักฐานแสดงถึงการดำเนินการและเพื่อความโปร่งใส	

ตาราง 15 การดำเนินการต่าง ๆสำหรับการใช้และเปิดเผยข้อมูลส่วนบุคคล

14. หลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ

มีหลักเกณฑ์สำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่เกี่ยวข้อง ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ	
2.	การอนุมัติหรือการรับรองเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	
3.	การได้รับการยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และสามารถโอนย้ายข้อมูลไปยังต่างประเทศได้	

ตาราง 16 หลักเกณฑ์สำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศที่เกี่ยวข้อง

<u>ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ</u>

การพิจารณาประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	พิจารณาว่ามีกฎหมายและมาตรการความมั่นคงปลอดภัยที่เกี่ยวข้อง หรือไม่ เช่น • กฎหมายการคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานจากกฎหมายที่เกี่ยวข้องของประเทศปลายทาง • การรักษาความมั่นคงปลอดภัยของประเทศ • กฎหมายอาญา • การเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานของรัฐ • กฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล • มาตรฐานในการรักษาความมั่นคงปลอดภัยของข้อมูล • กฎเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ • มาตรการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลกรณีที่ข้อมูลส่วนบุคคลถูกละเมิด	
2.	พิจารณาจากการมีหน่วยงานหรือองค์กรในประเทศปลายทางที่มีอำนาจหน้าที่ในการบังคับใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) และมีอำนาจหน้าที่ในการช่วยเหลือเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของตนเอง รวมทั้งอำนาจหน้าที่ในการร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรไทย	

การพิจารณาประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
3.	พิจารณาจากข้อผูกพันระดับนานาชาติของประเทศหรือองค์การระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล (ถ้ามี) เช่น การมีอนุสัญญาที่มีผลผูกพันทางกฎหมาย หรือการเข้าร่วมในระบบพหุภาคีหรือภูมิภาค ซึ่งมีผลในการควบคุมและป้องกันการใช้ข้อมูลส่วนบุคคล	

ตาราง 17 การพิจารณาประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลที่มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

<u>การได้รับการยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสามารถโอนย้ายข้อมูลไปยังต่างประเทศได้</u>

มีการพิจารณาการการได้รับการยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสามารถโอนย้ายข้อมูลไปยังต่างประเทศดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	เป็นการปฏิบัติตามกฎหมาย	
2.	ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยองค์กรได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว	
3.	เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใชในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น	
4.	เป็นการกระทำตามสัญญาระหว่างคณะทำงานข้อมูลส่วนบุคคล (ผู้แทนส่วนต่าง ๆ) กับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล	
5.	เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้	
6.	เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ	

ตาราง 18 การพิจารณาการการได้รับการยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและสามารถโอนย้ายข้อมูลไปยังต่างประเทศ

15. การจัดส่งข้อมูลส่วนบุคคลไปยังต่างประเทศ

กรณีเป็นหน่วยงานในต่างประเทศที่มีอำนาจหน้าที่ที่เกี่ยวข้องร้องขอให้จัดส่ง

กรณีเป็นหน่วยงานในต่างประเทศที่มีอำนาจหน้าที่ที่เกี่ยวข้องร้องขอให้จัดส่ง มีการดำเนินการ ดังต่อไปนี้ หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	มีการระบุวัตถุประสงค์ของการจัดส่งข้อมูล หรือไม่	
2.	มีการดำเนินการพิสูจน์ตัวตนหน่วยงานปลายทางในต่างประเทศนั้น หรือไม่ ว่าเป็นหน่วยงานใด และมีอำนาจหน้าที่ที่เกี่ยวข้องอย่างไร	
3.	มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับการจัดส่งข้อมูลนั้น หรือไม่	
4.	มีการประเมินความพร้อมที่จะดำเนินการจัดส่งไปยังหน่วยงานปลายทางตามหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศ ที่กำหนดไว้ หรือไม่มีการแจ้งผลการประเมินให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ หรือไม่ (ไม่ว่าผลการประเมิน จะสามารถดำเนินการหรือไม่ก็ตาม)	
5.	มีการขออนุมัติจากผู้มีอำนาจหน้าที่ภายในองค์กรก่อนการจัดส่ง หรือไม่	
6.	มีการใช้มาตรการการจัดส่งที่มีความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลรั่วไหลในระหว่างทาง หรือไม่	
7.	มีการบันทึกหลักฐานแสดงการจัดส่งข้อมูลนั้นไปยังต่างประเทศ หรือไม่	
8.	มีการแจ้งหรือพิจารณาการจัดส่งข้อมูลไปยังต่างประเทศโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือไม่	

ตาราง 19 กรณีเป็นหน่วยงานในต่างประเทศที่มีอำนาจหน้าที่ที่เกี่ยวข้องร้องขอให้จัดส่ง

16. การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอก

การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอกมีการดำเนินการ ดังต่อไปนี้หรือไม่		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	หน่วยงานภายนอกที่ร้องขอข้อมูลส่วนบุคคลเป็นหน่วยงานดังนี้หรือไม่ • เป็นหน่วยงานราชการ หน่วยงานอิสระที่มีอำนาจตามกฎหมาย หรือเป็นประกาศที่มีผลบังคับทางกฎหมายให้ดำเนินการ	
2.	การแจ้งให้ทราบ หรือพิจารณาการร้องขอข้อมูลจากหน่วยงานภายนอก โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือไม่	
3.	กรณีเป็นหมายศาล หรือหนังสือราชการที่เป็นลายลักษณ์อักษร (ซึ่งมาจากหน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้อง) หนังสือหรือเอกสารดังกล่าวมีรายละเอียดดังนี้หรือไม่ • หน่วยงานผู้ร้องขอ • อำนาจหน้าที่ตามกฎหมาย • วัตถุประสงค์ของการขอข้อมูล • ชื่อเจ้าหน้าที่ ตำแหน่ง วันที่ และตราประทับ (ถ้ามี)	
4.	กรณีไม่มีเป็นหนังสือราชการ (เช่น การเดินทางมาด้วยตนเองที่องค์กรฯ หรือการส่งเป็นอีเมลมาร้องขอ) มีการพิสูจน์ตัวตนหน่วยงานผู้ร้องขอก่อนดำเนินการให้ตามคำร้องขอหรือไม่ มีการสอบถามถึงอำนาจหน้าที่ตามกฎหมายของหน่วยงานดังกล่าวหรือไม่มี การสอบถามถึงวัตถุประสงค์ของร้องขอข้อมูลหรือไม่ กรณีการส่งเป็นอีเมลมาร้องขอ อีเมลนั้นเป็นอีเมลของ หรือมาจากหน่วยงานผู้มีอำนาจหรือไม่ มีการปฏิเสธการรับเรื่องสำหรับการร้องขอที่มาจากอีเมลสาธารณะหรือไม่มีการขอขอสำเนาบัตรประจำตัวของผู้ที่ร้องขอ (ซึ่งอาจเป็นบัตรข้าราชการ บัตรประชาชน หรือเอกสารยืนยันตัวตนอื่น ๆ) และลงลายมือชื่อด้วย หรือไม่	
5.	เมื่อพิจารณาและเห็นว่าสามารถดำเนินการให้ได้ มีการจัดทำบันทึกเพื่อเป็นหลักฐานการส่งมอบข้อมูลและเพื่อความโปร่งใส หรือไม่ มีการใช้มาตรการการจัดส่งที่มีความมั่นคงปลอดภัยเพื่อป้องกันข้อมูลส่วนบุคคลรั่วไหล หรือไม่ สำหรับคนการส่งเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ มีการใช้การเข้ารหัสข้อมูลก่อนการจัดส่ง หรือไม่	

ตาราง 20 การร้องขอข้อมูลส่วนบุคคลจากหน่วยงานภายนอกมีการดำเนินการ

17. การจ้างผู้ให้บริการภายนอกที่มีสัญญาหรือข้อตกลงการให้บริการ

ดูแนวทางการตรวจสอบได้ในหัวข้อ **ผู้ประมวลผลข้อมูลส่วนบุคคล / การทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคล**

18. การพิจารณาความเสี่ยงที่เกี่ยวข้องกับงานจ้างผู้ให้บริการภายนอกและกำหนดมาตรการที่จำเป็นลงสัญญา หรือข้อตกลงการให้บริการเพื่อให้ผู้ให้บริการภายนอกปฏิบัติตาม

สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก ให้ตรวจสอบงานจ้างดังนี้		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	มีการกำหนดลักษณะงานจ้างให้ชัดเจน หรือไม่	
2.	มีการกำหนดวัตถุประสงค์ของงานจ้าง หรือไม่	
3.	มีการประเมินความเสี่ยงที่เกี่ยวข้องกับการละเมิดสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล แยกตามวัตถุประสงค์ของงานจ้าง ที่กำหนดไว้หรือไม่ (ความเสี่ยงเหล่านั้นจะส่งผลกระทบต่อข้อมูลส่วนบุคคลที่องค์กรฯ จะต้องให้แก่ผู้ให้บริการภายนอก โดยรวมแล้ว เป็นความเสี่ยงที่ทำให้ไม่บรรลุวัตถุประสงค์ตามที่ต้องการ)	
4.	มีการกำหนดมาตรการที่จำเป็นเพื่อรองรับความเสี่ยงเหล่านั้น หรือไม่	
5.	มีการบรรจุมาตรการเหล่านั้นลงในสัญญาหรือข้อตกลงการให้บริการ หรือไม่	

ตาราง 21 สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก

19. การดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก ให้ตรวจสอบงานจ้างดังนี้		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	พิจารณาตรวจสอบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ว่าเป็นไปตามเงื่อนไขที่ต้องให้บริการ หรือสามารถปฏิเสธคำร้องขอได้ โดยพิจารณาจากหลักเกณฑ์ที่กำหนดไว้ใน หลักเกณฑ์การดำเนินการเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอใช้สิทธิ	
2.	มีการบันทึกคำขอใช้สิทธิโดยเจ้าของข้อมูลส่วนบุคคลไว้หรือไม่ บันทึกรายละเอียดของการดำเนินการไว้หรือไม่ กรณีที่มีการปฏิเสธ มีการบันทึกสาเหตุของการปฏิเสธไว้หรือไม่	
3.	ข้อมูลที่บันทึกไว้มีความครบถ้วน และสมบูรณ์หรือไม่	
4.	มีการบันทึกระยะเวลาการดำเนินการไว้หรือไม่ ระยะเวลาดำเนินการเป็นไปตามนโยบายที่องค์กรกำหนดไว้ใน การให้บริการหรือไม่	

ตาราง 22 สำหรับงานจ้างประมวลผลข้อมูลส่วนบุคคลที่จะมีการจ้างผู้ให้บริการภายนอก

20. การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

พิจารณาตรวจสอบการแจ้งและการจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ดังนี้

พิจารณาตรวจสอบการแจ้งและการจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ดังนี้		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	มีการบันทึกการแจ้งเหตุละเมิดความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรไว้หรือไม่ บันทึกรายละเอียดของการดำเนินการไว้หรือไม่ ข้อมูลที่บันทึกไว้มีความครบถ้วนและสมบูรณ์หรือไม่	
2.	มีการวิเคราะห์หาสาเหตุที่เกิดขึ้น และแนวทางในการรับมือกับเหตุที่เกิดขึ้นหรือไม่ ได้มีการดำเนินการตามแนวทางในการรับมือที่กำหนดไว้หรือไม่	

ตาราง 23 พิจารณาตรวจสอบการแจ้งและการจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

พิจารณากรณีเหตุละเมิดมีผลกระทบสูง ดังนี้		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	มีการแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพิจารณา และตัดสินใจดำเนินการต่างๆ ตามความจำเป็นหรือไม่ ผู้บริหารระดับสูงทราบเรื่องที่เกิดขึ้นหรือไม่ และได้มีการพิจารณามอบหมายให้ดำเนินการต่างๆ หรือไม่	
2.	มีการกำหนดแนวทางในการเยียวยาเหตุที่เกิดขึ้น และ การดำเนินการต่าง ๆ ตามความจำเป็นหรือไม่	
3.	มีการแจ้งภายใน 72 ชั่วโมงนับตั้งแต่มีการรายงานเหตุละเมิดไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ได้รับทราบหรือไม่ การแจ้งมีรายละเอียดดังนี้หรือไม่ 1. คำอธิบายลักษณะของการละเมิดข้อมูลส่วนบุคคล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณและปริมาณข้อมูลที่เกี่ยวข้อง 2. ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบ หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 3. ผลกระทบที่อาจจะเกิดขึ้นได้จากเหตุละเมิด 4. แนวทางการเยียวยาต่อเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด (ถ้ามี) 5. กรณีที่ไม่อาจแจ้งเหตุได้ภายใน 72 ชั่วโมง องค์กรจะต้องแจ้งเหตุผลของการดำเนินการที่ล่าช้า	
4.	มีการแจ้งรายละเอียดดังนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบได้รับทราบหรือไม่ 1. คำอธิบายลักษณะของการละเมิดข้อมูลส่วนบุคคล 2. ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 3. ผลและความเสียหายที่อาจจะเกิดขึ้นจาก การละเมิดข้อมูลส่วนบุคคล 4. แนวทางการเยียวยา	
5.	มีการจัดทำรายงานสรุปเหตุที่เกิดขึ้นและแนวทาง การดำเนินการต่อไป (After Action Report) หรือไม่	
6.	ได้มีการจัดส่งรายงานให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและผู้บริหารระดับสูงได้พิจารณา เพื่อมอบหมายหรือให้ข้อคิดเห็นต่าง ๆ สำหรับการดำเนินการหรือไม่	

ตาราง 24 พิจารณากรณีเหตุละเมิดมีผลกระทบสูง

21. การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล

พิจารณาประเมินการจัดเก็บรักษาและระยะเวลาในการจัดเก็บไว้ว่ามีความเหมาะสมหรือไม่ ดังนี้

พิจารณาประเมินการจัดเก็บรักษาและระยะเวลาในการจัดเก็บไว้ว่ามีความเหมาะสมหรือไม่ ดังนี้		
หัวข้อ		ผลการตรวจสอบ/หลักฐาน
1.	ข้อมูลที่เก็บรักษาไว้จัดเก็บไว้เท่าที่จำเป็นหรือไม่ สอดคล้องกับวัตถุประสงค์หรือไม่ มีข้อมูลใดที่ไม่จำเป็นต้องจัดเก็บรักษาไว้หรือไม่	
2.	ข้อมูลที่เก็บรักษาไว้ เก็บรักษาไว้ตามระยะเวลาที่ได้แจ้ง	
3.	ให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบในช่วงที่เก็บรวบรวมข้อมูลส่วนบุคค ลหรือไม่	
4.	ข้อมูลที่เก็บรักษาไว้หมดความจำเป็นที่จะต้องเก็บรักษาไว้หรือไม่ และได้มีการลบทำลายเมื่อหมดความจำเป็นหรือไม่	
5.	มีการกำหนดระยะเวลาสำหรับการตรวจสอบเพื่อทำลายข้อมูลส่วนบุคคลหรือไม่ เช่น ดำเนินการตรวจสอบในทุก ๆ สิ้นปี เพื่อทำลายตามความจำเป็น	
6.	ข้อมูลประเภทเอกสารมีการจัดเก็บไว้ในสถานที่ที่มีความปลอดภัยหรือไม่	
7.	ข้อมูลที่มีความอ่อนไหวและเป็นข้อมูลอิเล็กทรอนิกส์ มีการเข้ารหัสเพื่อจัดเก็บข้อมูลไว้หรือไม่	
8.	มีการปฏิบัติตามขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลตามชั้นความลับที่องค์กรกำหนดไว้หรือไม่ เพื่อป้องกันข้อมูลที่มีการจัดเก็บไว้	

ตาราง 25 พิจารณาประเมินการจัดเก็บรักษาและระยะเวลาในการจัดเก็บ

22. การจัดเก็บรักษาและระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล

การจำหน่ายออกและลบทำลายข้อมูลส่วนบุคคลขององค์กร สอดคล้องกับเงื่อนไขดังต่อไปนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	เมื่อครบระยะเวลาการจัดเก็บที่ได้แจ้งให้เจ้าของข้อมูลได้รับทราบ หรือตามที่ระบุไว้ในสัญญา หรือครบกำหนดระยะเวลาตามที่กฎหมายกำหนดไว้	
2.	เมื่อครบระยะเวลาการจัดเก็บที่กำหนดไว้และไม่มีข้อกำหนดทางกฎหมายใดระบุให้จัดเก็บเพิ่มเติม	
3.	เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการใช้งานอีกต่อไป	
4.	เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ หรือได้ถอนความยินยอม และองค์กรไม่มีอำนาจตามกฎหมายใดที่จะจัดเก็บรักษาไว้ได้อีกต่อไป	
5.	เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผล และองค์กรไม่สามารถปฏิเสธคำคัดค้านดังกล่าวได้	
6.	เมื่อพบว่าข้อมูลส่วนบุคคลที่องค์กรจัดเก็บไว้ไม่ชอบด้วยกฎหมาย จะด้วยเหตุผลใดก็ตามที่ได้รวบรวมหรือจัดเก็บข้อมูลนั้นมา	

ตาราง 26 การจำหน่ายออกและลบทำลายข้อมูลส่วนบุคคลขององค์กร

การดำเนินการจำหน่ายออกข้อมูลส่วนบุคคลขององค์กร มีการดำเนินการดังนี้หรือไม่		
	หัวข้อ	ผลการตรวจสอบ/หลักฐาน
1.	จัดทำทะเบียนและบันทึกรายละเอียดของการทำลายข้อมูลนั้น (ข้อมูลที่ต้องทำลาย ประเภทของข้อมูล จำนวนหรือปริมาณของข้อมูลที่ถูกทำลาย วิธีการทำลาย วันเวลาที่ทำลาย สถานที่ที่ทำลาย ผู้ควบคุม การทำลาย ผู้ดำเนินการทำลาย ทำลายสำเร็จหรือไม่)	
2.	ขออนุมัติการทำลายเอกสารจากผู้ควบคุมข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาการทำลาย	
3.	ดำเนินการทำลายตามวิธีการที่องค์กรกำหนดไว้	
4.	รายงานผลการทำลายให้ผู้ควบคุมข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือผู้ที่ได้รับมอบหมายให้เป็นผู้พิจารณาการทำลาย ได้รับทราบ	

ตาราง 27 การดำเนินการจำหน่ายออกข้อมูลส่วนบุคคลขององค์กร