เผยแพร่ ณ วันที่ 28 เมษายน 2564

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจธนาคาร สมาคมธนาคารไทย

(Guideline on Personal Data Protection for Thai Banks)

คำสงวนสิทธิ์ : *สมาคมธนาคารไทยจัดทำ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจ ธนาคารนี้ เพื่อใช้เป็นข้อเสนอแนะสำหรับธนาคารสมาชิกนำไปพิจารณาเป็นแนวปฏิบัติเบื้องต้นตามที่ธนาคารสมาชิกเห็นสมควรเพื่อรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไป ทั้งนี้ สมาคมธนาคารไทยขอสงวนสิทธิในการแก้ไขปรับปรุงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับธนาคารพาณิชย์ไทยนี้ ดังกล่าวได้ ในกรณีที่มีการแก้ไขกฎหมายหรือมีการประกาศใช้กฎหมายลำดับรอง หรือมีการแก้ไขเปลี่ยนแปลงแนวทางการปฏิบัติภายในภาคธุรกิจของแต่ละธนาคาร เพื่อให้แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลภาคธุรกิจ ธนาคารมีความสมบูรณ์ และ ธนาคารสมาชิกสามารถนำไปพิจารณาปรับใช้ได้อย่าง มีประสิทธิภาพ”*

สารบัญ

1. บทนำ 5

2. คำนิยาม 8

3. ขอบเขตของข้อมูลส่วนบุคคลและการจำแนกข้อมูลส่วนบุคคล (Personal Data Scope and Classification) 11

3.1 การระบุข้อมูลส่วนบุคคล (Identifying Personal Identifiable Information) 11

3.1.1 ตัวอย่างของข้อมูลที่เป็นข้อมูลส่วนบุคคล 12

3.1.2 ตัวอย่างของข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล 13

3.2 แนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) 13

3.2.1 การกำหนดเจ้าของข้อมูล (Information Owner/Data Owner) 13

3.2.2 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล (Data Classification) 13

3.2.3 ปัจจัยในการกำหนดผลกระทบที่อาจเกิดขึ้นต่อการรักษาความลับของข้อมูลส่วนบุคคล (Factors for Determining PII Confidentiality Impact Levels) 17

4. หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles) 19

4.1 **Principle 1** : ("Lawfulness, Fairness, and Transparency") 19

4.2 **Principle 2** : ("Purpose Limitation") 20

4.3 **Principle 3** : ("Data Minimisation") 21

4.4 **Principle 4** : ("Accuracy") 21

4.5 **Principle 5** : ("Storage Limitation") 22

4.6 **Principle 6** : ("Integrity and Confidentiality") 22

4.7 **Principle 7** : ("Accountability") 23

5. การเก็บรวบรวมข้อมูลส่วนบุคคล 23

5.1 วัตถุประสงค์ในการเก็บรวบรวมข้อมูล 23

5.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล 24

5.2.1 ฐานความยินยอม (Consent) 24

5.2.2 ฐานสัญญา (Contract) 25

5.2.3 ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest) 27

5.2.4 ฐานภารกิจของรัฐ (Public Task) 27

5.2.5 ฐานประโยชน์อันชอบธรรม (Legitimate Interest) 28

5.2.6 ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) 35

5.2.7 ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research) 36

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5.3 ความยินยอม (Consent) 36

5.4 ข้อมูลอ่อนไหว (Sensitive Personal Data) 47

5.5 การประกาศความเป็นส่วนตัว (Privacy Notice) 50

6. การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage and Data Disclosure) 58

6.1 แนวปฏิบัติในการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการในประเทศ 60

6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Cross-border data transfer) 60

6.2.1 ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ 61

6.2.2 กรณีที่ได้รับการยกเว้นตามกฎหมาย 62

6.2.3 กรณีที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Transfers Subject to Appropriate Safeguards) 63

6.3 แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ 64

6.4 การประมวลผลข้อมูลเพื่อวัตถุประสงค์เฉพาะ 65

6.4.1 การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง (Direct Marketing) 65

7. การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บ (Data Retention) 68

7.1 แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล 69

8. การลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction) 70

8.1 แนวปฏิบัติเกี่ยวกับการทำข้อมูลนิรนาม (Data Anonymization) 71

9. แนวปฏิบัติเกี่ยวกับข้อมูลที่มีการเก็บอยู่ก่อนแล้ว 73

10. แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคล 73

10.1 สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”) 74

10.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”) 74

10.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”) 76

10.4 สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล (“Right to Erasure” or “Right to be Forgotten”) 77

10.5 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (“Right to Restriction of Processing”) 78

10.6 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”) 79

10.7 สิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”) 80

11. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Guideline on Data Controller and Data Processor Roles and Responsibilities) 81

11.1 การระบุสถานะในการคุ้มครองข้อมูลส่วนบุคคลของธนาคาร 81

11.2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller Roles and Responsibilities) 83

11.3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Roles and Responsibilities) 87

12. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) 88

12.1 การแต่งตั้งและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล 88

12.2 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Responsibility of DPO) 89

13. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) 90

13.1 ความแตกต่างระหว่าง Data Protection Impact Assessment (DPIA) กับ Privacy Impact Assessment (PIA) 90

13.2 แนวปฏิบัติเกี่ยวกับการจัดทำ DPIA 91

14. แนวปฏิบัติเกี่ยวกับ Three Lines of Defense สำหรับการบริหารจัดการข้อมูลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล 97

15. เหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach) 99

17. Appendix A 113

1. Product: Saving Accounts 113

2. Product: Loan Process 118

3. Product: Mobile Banking (Registration Process) 121

4. Service: Internet Banking (Purchase Product Process) 124

5. Product: Payment 127

6. Product: Credit Card 129

18. Appendix B 132

18.1 ตัวอย่างกระบวนการปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคล 132

19. Appendix C 133

19.1 การจัดทำข้อมูลนิรนาม (Data Anonymization) 133

19.2 การแฝงข้อมูล (Data Pseudonymisation) 134

19.3 การเข้ารหัสข้อมูล (Data Encryption) 135

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

1. บทนำ

- การคุ้มครองข้อมูลส่วนบุคคลกับกลุ่มธนาคารไทย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) จะมีผลบังคับใช้อย่างสมบูรณ์ในวันที่ 1 มิถุนายน พ.ศ. 2564 ซึ่งสมาคมธนาคารไทย (Thai Bankers’ Association) ได้เห็นถึงความสำคัญ ของการกำหนดแนวทางในการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลในกลุ่มธนาคาร เพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทยนั้นมีการอ้างอิงกับกฎหมายของสหภาพยุโรป ที่เรียกกันว่า “GDPR” (EU General Data Protection Regulation) ที่มีตัวบทกฎหมายที่มีความชัดเจนและครอบคลุม ดังนั้นเอกสารแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของธนาคารไทย (Guideline on Personal Data Protection for Thai Banks) ฉบับนี้ จึงมีการนำเนื้อหาบางส่วนของ GDPR มาปรับใช้เพื่อเป็นแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล อีกทั้ง มีการยกตัวอย่างแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ เพื่อให้ผู้อ่านสามารถเข้าใจถึงการนำตัวบทกฎหมายไปปฏิบัติได้ดียิ่งขึ้น

มาตรการในการคุ้มครองข้อมูลส่วนบุคคล มีการมุ่งเน้นถึง หน้าที่และความรับผิดชอบของนิติบุคคลในการกระทำการใดๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล อันเนื่องมาจากในประเทศไทย มีผู้ประกอบการจำนวนมากทำการติดต่อและรับส่งข้อมูลส่วนบุคคลกัน ทั้งการรับส่งภายในกันเองภายในองค์กรและภายนอกองค์กร อีกทั้งยังมีการส่งข้อมูลส่วนบุคคลออกนอกประเทศ มีการนำข้อมูลไปเผยแพร่เพื่อประโยชน์ส่วนตนโดยไม่ได้รับอนุญาต หรือมีการติดต่อไปยังเจ้าของข้อมูลส่วนบุคคลมากจนเกินความจำเป็น จนอาจเป็นการรบกวนความเป็นส่วนตัว ซึ่งข้อมูลดังกล่าว มีทั้งข้อมูลที่เป็นข้อมูลทางธุรกิจ และข้อมูลส่วนบุคคล (นั่นก็คือข้อมูลที่เกี่ยวข้องโดยตรงกับบุคคลที่ทำให้สามารถระบุตัวตนได้ ไม่ว่าทางตรงหรือทางอ้อม) การกระทำใดๆ กับข้อมูลส่วนบุคคลนั้น อาจมีความเสี่ยงที่จะเป็นการกระทำอันละเมิดหรือกระทบต่อสิทธิและเสรีภาพของบุคคลได้ ดังนั้น จึงต้องมีกฎหมาย กฎเกณฑ์ต่างๆ มาควบคุมและจำกัดการใช้ข้อมูลส่วนบุคคล รวมถึงบทลงโทษสำหรับการละเมิดกฎข้อบังคับต่างๆ เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งสิทธิความเป็นส่วนตัวให้ดียิ่งขึ้น ผู้ประกอบการจึงต้องมีการใช้ข้อมูลอย่างระมัดระวังมากขึ้น มิให้การประมวลผลข้อมูลส่วนบุคคลเป็นการละเมิดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล ซึ่งเป็นหน้าที่ของผู้ประกอบการที่ต้องจัดให้มาตรการที่ทำให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการคุ้มครอง มีการบริหารจัดการข้อมูลอย่างเหมาะสม

- เป้าหมายและวัตถุประสงค์ของเอกสารฉบับนี้

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของธนาคารไทย (Guideline on Personal Data Protection for Thai Banks) มีวัตถุประสงค์เพื่อให้มั่นใจว่าธนาคารไทยตระหนักและเข้าใจถึงการคุ้มครองข้อมูลส่วนบุคคลและเพื่อเป็นแนวทางในการนำ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ไปถือปฏิบัติโดยให้เป็น

มาตรฐานเดียวกันในกลุ่มธนาคารไทย เอกสารฉบับนี้มีกลุ่มเป้าหมายให้กับผู้จัดทำนโยบายของธนาคาร เพื่อให้ง่ายต่อการนำไปพัฒนาเป็นร่างนโยบายและวิธีปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของแต่ละธนาคารให้เหมาะสมและสอดคล้องกับความเสี่ยงและวิธีการดำเนินธุรกิจของแต่ละธนาคารเองได้อย่างเหมาะสม

- การใช้แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของธนาคารไทยฉบับนี้ สามารถสรุปเนื้อหาหลัก ได้ดังต่อไปนี้
  1) หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Principle Relating to Personal Data Protection)
  2) แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล แบ่งตามวงจรชีวิตของข้อมูล (Data Life Cycle) ได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคล (Data Collection), การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage/Disclose/Transfer), การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บรักษา (Data Retention) และการลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction)
  3) สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)
  4) แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Controller and Data Processor Obligation) รวมทั้งหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer Roles and Responsibilities)
  5) ภาคผนวก ได้แก่ ตัวอย่างการประมวลผลข้อมูลส่วนบุคคลของธนาคาร

- ข้อจำกัดในการปฏิบัติงานและข้อจำกัดของเอกสารฉบับนี้

บริษัท ดีล้อย ทู้ช โธมัทสุ ไชยยศ ที่ปรึกษา จำกัด (“บริษัทที่ปรึกษา”) มีข้อจำกัดในการปฏิบัติงานเพื่อจัดทำแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของสมาคมธนาคารไทย ดังต่อไปนี้

- เอกสารฉบับนี้อ้างอิงตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเป็นหลัก รวมถึงกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศที่มีข้อกำหนดที่ใกล้เคียงกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทย และกฎหมายที่เกี่ยวข้องกับธนาคาร
- เอกสารฉบับนี้ มีขอบเขตการศึกษา วิเคราะห์ และตีความ จากประสบการณ์และจากฐานข้อมูลที่น่าเชื่อถือ ทั้งในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลและผลิตภัณฑ์หรือบริการที่เกี่ยวข้องของธนาคาร อย่างไรก็ตาม ข้อมูลอ้างอิงดังกล่าวเป็นข้อมูลที่มี ณ เวลาใดเวลาหนึ่ง และ ธนาคารควรตระหนักด้วยว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่กำลังพัฒนาและมีการปรับปรุงเปลี่ยนแปลงอยู่ อย่างรวดเร็ว ดังนั้น เนื้อหาหลายประการอาจมี

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ความล้าสมัยหรือไม่เหมาะสมในหลายสถานการณ์เมื่อเวลาผ่านไป หรือรายการอ้างอิงใดๆ ของเนื้อหาอาจมีการเปลี่ยนแปลง สูญหายได้เมื่อถึงเวลาที่ท่านได้อ่านเอกสารฉบับนี้ ดังนั้น ธนาคารจึงอาจจำเป็นต้องได้รับคำปรึกษาจากผู้เชี่ยวชาญในเรื่องดังกล่าวโดยตรง

- บริษัทที่ปรึกษาไม่ได้ปฏิบัติงานด้านการให้คำปรึกษาทางกฎหมาย ดังนั้นจึงไม่สามารถรับรองความถูกต้องของครบถ้วนของเนื้อหา รวมถึงไม่สามารถให้คำรับรองหรือรับประกันใดๆทั้งสิ้นของเนื้อหาในเอกสารฉบับนี้ได้ และบริษัทที่ปรึกษาจะไม่รับผิดชอบต่อความสูญเสีย หรือเสียหายใดๆ ที่อ้างว่าเกิดขึ้นจากการปฏิบัติตามเนื้อหาของเอกสารฉบับนี้ ไม่ว่ากรณีใดๆ ทั้งสิ้น

2. คำนิยาม

รายการ	คำอธิบายรายการ
การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data)	หมายถึง การดำเนินการหรือชุดการดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบ จัดโครงสร้าง การอัปเดตหรือการแก้ไข การดึงข้อมูล การใช้ การเปิดเผยด้วยการส่งต่อ เผยแพร่ หรือ การกระทำใดๆ เพื่อให้พร้อมใช้งาน การใช้ การรวม การบล็อก การลบหรือการทำลายข้อมูล
การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิด ความเสียหาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต
การลบข้อมูล (Data Deletion)	หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใด ๆ
การทำข้อมูลนิรนาม (Data Anonymization)	หมายถึงกระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
กลุ่มธุรกิจทางการเงิน (Financial Business Group)	หมายความว่า กลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลกลุ่มธุรกิจทางการเงินและกฎเกณฑ์ที่เกี่ยวข้อง
ข้อมูลนิรนาม (Anonymized Data)	หมายถึง ข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
ข้อมูลส่วนบุคคล (Personal Data)	หมายถึง ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ ตามคำนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ข้อมูลส่วนบุคคล (Personal Identifiable Information หรือ PII)	หมายถึง ข้อมูลที่เกี่ยวกับตัวบุคคลซึ่งทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม ตามคำนิยามของ National Institutional of Standard and Technology (NIST)
ข้อมูลอ่อนไหว (Sensitive Personal Data)	หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และมีความละเอียดอ่อนและมีความสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม หรือเป็นข้อมูลอื่นใดซึ่งอาจทำให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
คณะกรรมการ (Personal Data Protection Committee)	หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง บุคคลใดๆ ที่ข้อมูลใดๆทำให้สามารถระบุตัวตนนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม
บริษัทในเครือ (Affiliated Company)	หมายถึง บริษัท หรือนิติบุคคลใด ๆ ซึ่งมีความสัมพันธ์กับบริษัทมหาชนจำกัด หรือบริษัทเอกชนบริษัทใดบริษัทหนึ่งหรือหลายบริษัท ในลักษณะดังต่อไปนี้ (1) บริษัทหนึ่งมีอำนาจควบคุมเกี่ยวกับการแต่งตั้งและถอดถอนกรรมการ ซึ่งมีอำนาจจัดการทั้งหมดหรือโดยส่วนใหญ่ของอีกบริษัทหนึ่ง (2) บริษัทหนึ่งถือหุ้นในอีกบริษัทหนึ่งเกินกว่าร้อยละห้าสิบของหุ้นที่ออกจำหน่ายแล้ว ในกรณีที่บริษัทแรกและ/หรือบริษัทในเครือบริษัทเดียวหรือหลายบริษัท หรือบริษัทแรกและ/หรือบริษัทในเครือในลำดับชั้นแรกและ/หรือในชั้นต่อ ๆ ไป บริษัทเดียวหรือหลายบริษัทถือหุ้นของบริษัทใดมีจำนวนรวมกันเกินกว่าร้อยละห้าสิบของหุ้นที่ออกจำหน่ายแล้วให้ถือว่าบริษัทนั้นเป็นบริษัทในเครือของบริษัทแรกด้วย
โปรไฟลิ่ง (Profiling)	รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินลักษณะเกี่ยวกับบุคคลบางประการ โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล สถานะทางการเงินของบุคคล สุขภาพของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล
ผลิตภัณฑ์ (Product)	หมายถึง ผลิตภัณฑ์และบริการทางการเงินทุกประเภทที่ผู้ให้บริการเป็นผู้ออก ผู้แนะนำ หรือผู้ขาย ซึ่งรวมถึงผลิตภัณฑ์ที่อยู่ภายใต้การกำกับของหน่วยงานอื่น เช่น ตราสารหนี้ กองทุนรวม ประกันวินาศภัย และประกันชีวิต
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล [เอกสารฉบับนี้อาจมีการใช้คำว่า ผู้ควบคุมข้อมูลแทนคำว่าผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่

	เป็นผู้ควบคุมข้อมูลส่วนบุคคล [เอกสารฉบับนี้อาจมีการใช้คำว่า ผู้ประมวลผลข้อมูลแทนคำว่าผู้ประมวลผลข้อมูลส่วนบุคคล]
ลูกค้า (Customer)	หมายถึง บุคคลธรรมดาและนิติบุคคลซึ่งใช้ผลิตภัณฑ์อยู่ในปัจจุบัน และให้หมายความรวมถึงผู้ติดต่อสอบถามข้อมูลผลิตภัณฑ์ ผู้ที่รับทราบผลิตภัณฑ์ผ่านสื่อต่าง ๆ และผู้ที่ได้รับการเสนอหรือชักชวนจากผู้ให้บริการเพื่อให้ซื้อผลิตภัณฑ์
สำนักงานคุ้มครองข้อมูลส่วนบุคคล	หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Office of the Personal Data Protection Committee)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

3. ขอบเขตของข้อมูลส่วนบุคคลและการจำแนกข้อมูลส่วนบุคคล (Personal Data Scope and Classification)

3.1 การระบุข้อมูลส่วนบุคคล (Identifying Personal Identifiable Information)

"ข้อมูลส่วนบุคคล" (Personal Data) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ "เจ้าของข้อมูลส่วนบุคคล" (Data Subject) หมายความว่า บุคคลผู้ที่ข้อมูลส่วนบุคคลสามารถระบุไปถึง

เพื่อเป็นการอธิบายคำว่าข้อมูลส่วนบุคคล National Institutional of Standard and Technology ("NIST") ได้ให้คำนิยามของ Personal Identifiable Information (PII) หมายถึง ข้อมูลที่เกี่ยวกับตัวบุคคลซึ่งทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม ซึ่งความสามารถในการระบุตัวบุคคลสามารถแบ่งได้เป็น 3 ลักษณะ อันได้แก่ ความสามารถในการแยกแยะ การติดตาม และ การเชื่อมโยง ตัวอย่างของ PII เช่น ชื่อ ที่อยู่ อีเมล ข้อมูลทางการเงิน ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น การเข้าถึง ใช้ หรือเปิดเผย PII โดยมิได้รับอนุญาตนั้นอาจก่อเกิดให้ผลกระทบทางลบกับทั้งเจ้าของข้อมูลส่วนบุคคล เช่น อาจถูกสวมรอยโดยคนร้ายและเอาข้อมูลไปแอบอ้างเพื่อประโยชน์บางประการ อาจทำให้เกิดความอับอาย มีผลกระทบต่อความเป็นอยู่หรืออาจทำให้เกิดความเสียหายทางการเงิน เป็นต้น และเกิดผลกระทบทางลบกับผู้ควบคุมข้อมูลส่วนบุคคลเอง เช่น มีผลกระทบต่อชื่อเสียงขององค์กร ทำให้ความน่าเชื่อถือลดลง หรือต้องรับผิดทางกฎหมาย เป็นต้น

ความสามารถในการระบุไปยังเจ้าของข้อมูลส่วนบุคคลสามารถแบ่งได้เป็น 3 ลักษณะ

I. **การแยกแยะ (Distinguishability)** คือการที่ข้อมูลมีความสามารถในการระบุแยกแยะตัวบุคคลออกจากกันได้ ตัวอย่างเช่น ในชุดข้อมูล มี ชื่อ หมายเลขหนังสือเดินทาง หมายเลขประกันสังคม หรือข้อมูล Biometric ซึ่งข้อมูลดังกล่าวสามารถระบุตัวของเจ้าของข้อมูลได้ ในทางตรงกันข้าม หากชุดข้อมูลระบุเพียงคะแนนเครดิต (Credit score) นั้นไม่สามารถระบุไปยังตัวบุคคลได้ จำเป็นจะต้องมีข้อมูลเกี่ยวกับตัวบุคคลเพิ่มเติมจึงจะสามารถแยกแยะตัวบุคคลได้

II. **การติดตาม (Traceability)** คือการที่ข้อมูลสามารถถูกใช้ในการติดตาม เพื่อระบุลักษณะจำเพาะของบุคคลนั้นได้ ยกตัวอย่างเช่น พฤติกรรม กิจกรรมที่บุคคลนั้นกระทำ สถานะหรือการบันทึกการกระทำของผู้ใช้งานระบบที่ทำให้สามารถใช้ในการติดตามกิจกรรมของแต่ละบุคคลได้

III. **การเชื่อมโยง (Linkability)** คือการที่ข้อมูลมีคุณสมบัติในการเชื่อมโยงกันและระบุไปยังตัวบุคคลได้ ซึ่งแบ่งออกเป็น 2 ประเภท

- ข้อมูลที่ถูกเชื่อมโยงแล้ว (Linked Information) คือกรณีที่ข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลคนละชุด เมื่อใช้ข้อมูลทั้งสองชุดประกอบกันแล้วจะมีความสามารถในการระบุตัว

เจ้าของข้อมูลส่วนบุคคลได้ เช่น ข้อมูล PII สองชุดที่มีองค์ประกอบ PII ต่างกัน เมื่อมีบุคคลที่สามารถเข้าถึงชุดข้อมูลทั้งสองชุดได้ ก็จะสามารถเชื่อมโยงข้อมูลดังกล่าวในการระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงกรณีที่การเข้าถึงข้อมูลอื่นที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล หากฐานข้อมูลทั้งสองชุดอยู่ในระบบเดียวกันหรือระบบที่เกี่ยวข้องกันอย่างใกล้ชิด และไม่มีควบคุมการเข้าถึงอย่างมีประสิทธิภาพ กรณีนี้ถือเป็นข้อมูลที่ถูกเชื่อมโยงแล้วได้

- ข้อมูลที่อาจถูกเชื่อมโยงได้ (Linkable Information) คือกรณีที่ หากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูลอื่นแล้วก็จะสามารถระบุตัวบุคคลได้ โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมนั้นมาจากแหล่งข้อมูลอื่น โดยไม่อยู่ในระบบเดียวกันหรือระบบที่เกี่ยวข้องกันอย่างใกล้ชิด มีอยู่ในอินเทอร์เน็ต หรือแหล่งอื่น กรณีนี้เป็นข้อมูลที่ อาจถูกเชื่อมโยงได้

3.1.1 ตัวอย่างของข้อมูลที่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้คือตัวอย่างของข้อมูลที่อาจถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ชื่อ นามสกุล ชื่อกลาง
- เลขประจำตัวประชาชน หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง หมายเลขใบขับขี่ หมายเลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต
- ข้อมูลที่อยู่ อีเมล หมายเลขโทรศัพท์
- ข้อมูลอุปกรณ์ เช่น เลข IP address, MAC address, Cookie ID
- ข้อมูลที่เป็นลักษณะเฉพาะ เช่น รูปภาพใบหน้า
- ข้อมูลทางชีวมิติ (Biometric) ซึ่งเป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลแบบจำลองใบหน้า ข้อมูลแบบจำลองลายนิ้วมือ ฟิล์มเอกซเรย์ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม เป็นต้น
- ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน
  ข้อมูลเกี่ยวกับบุคคลที่เชื่อมโยงหรือถูกเชื่อมโยงกับหนึ่งในข้างต้น เช่น วันเกิด สถานที่เกิด น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งทางภูมิศาสตร์ (Location)

- เชื้อชาติ ศาสนา ความเชื่อ ลัทธิ เผ่าพันธุ์ ปรัชญา พฤติกรรมทางเพศ ความเห็นทางการเมือง ประวัติอาชญากรรม
- ข้อมูลการจ้างงาน ข้อมูลทางการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

3.1.2 ตัวอย่างของข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้คือตัวอย่างของข้อมูลที่ไม่ถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ข้อมูลจดทะเบียนบริษัท, ข้อมูลติดต่อทางธุรกิจ ที่ไม่ได้ระบุถึงตัวบุคคล เช่น ที่อยู่สำนักงาน, อีเมลบริษัท, หมายเลขโทรศัพท์สำนักงาน, หมายเลขแฟกซ์สำนักงาน
- ข้อมูลที่ไม่สามารถระบุถึงตัวบุคคลได้ เช่น ข้อมูลนิรนาม (Anonymized Data)
- ข้อมูลผู้ถึงแก่กรรม

3.2 แนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

3.2.1 การกำหนดหน่วยงานเจ้าของข้อมูล (Information Owner หรือ Data Owner หรือ Data Owners)

การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) ตามประกาศธนาคารแห่งประเทศไทย ได้กำหนดให้ธนาคารจะต้องทำการกำหนดหน่วยงานเจ้าของข้อมูล (Information Owner หรือ Data Owner หรือ Data Owners) คือ บุคคลหรือหน่วยงานที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง เพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย หน่วยงานเจ้าของข้อมูลจะต้องทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เป็นผู้รับผิดชอบในให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลอย่างปลอดภัยและเหมาะสม หน่วยงานเจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงาน ดังนั้นหน้าที่และความหมายของหน่วยงานเจ้าของข้อมูล (Data Owners) จึงแตกต่างกับคำว่า เจ้าของข้อมูลส่วนบุคคล (Data Subject) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลซึ่งมีความหมายตามที่ได้กล่าวไว้ในหัวข้อ 3.1

3.2.2 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล (Data Classification)

"การจำแนกข้อมูล" (Data Classification) หมายถึงกระบวนการที่เกี่ยวข้องกับการประเมินชุดข้อมูลกับการรักษาความปลอดภัยของข้อมูล อันได้แก่ ข้อมูลความลับ ข้อมูลอ่อนไหว ข้อมูลที่ต้องจัดให้มีเพื่อพร้อมใช้งาน และข้อมูลที่ต้องเปิดเผยตามข้อกำหนดของกฎหมาย เพื่อให้สามารถใช้ข้อมูล และกำหนดระดับการเปิดเผยอย่างเหมาะสม รวมถึงระดับการป้องกันความปลอดภัยของข้อมูล เพื่อเพิ่มความมั่นคงและความปลอดภัยของข้อมูล

การจำแนกข้อมูลเป็นกระบวนการที่ช่วยให้องค์กรรักษาความปลอดภัยของข้อมูลที่มีความอ่อนไหวหรือสำคัญให้อยู่ในระดับที่เหมาะสม ไม่ว่าข้อมูลจะถูกนำไปใช้งานหรือถูกเก็บในที่ใดก็ตาม การจำแนกข้อมูลถือเป็นจุดเริ่มต้นและเป็นพื้นฐานในการรักษาความเป็นส่วนตัวของข้อมูล ซึ่งองค์กรต้องทำการ

ตัดสินใจเกี่ยวกับการกระทำใด ๆ กับข้อมูล บนพื้นฐานของความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับองค์กร จะช่วยให้องค์กรประเมินความเสี่ยงในแต่ละประเภทของข้อมูลได้อย่างเหมาะสมยิ่งขึ้น ตัวอย่างการรักษาความปลอดภัยของข้อมูลในแต่ละประเภท เช่น ข้อมูลประเภทที่ "ถูกจำกัด" (Restricted) ควรได้รับการดูแลด้วยมาตรฐานที่สูงกว่าข้อมูลที่ "ไม่ถูกจำกัด" (Unrestricted) ที่ทุกคนในองค์กรสามารถเข้าถึงได้ เนื่องจากหากข้อมูลที่ถูกจำกัดเกิดการรั่วไหล อาจทำให้เกิดผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคลและองค์กรมากกว่าข้อมูลที่ไม่ถูกจำกัด

แนวปฏิบัติฉบับนี้ ได้นำหลักการการกำหนดผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดความปลอดภัยของข้อมูลส่วนบุคคลจาก National Institute of Standards and Technology (NIST) ในการกำหนดวัตถุประสงค์ด้านความปลอดภัย (Security Objective) ของข้อมูลออกเป็น 3 ด้าน ได้แก่

1. **การรักษาความลับของข้อมูล (Confidentiality)** คือ การจำกัดการเข้าถึงและการเปิดเผยข้อมูล รวมถึงการปกป้องความเป็นส่วนตัวและสิทธิของข้อมูล
2. **ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)** คือ การรักษาความปลอดภัยของข้อมูล จากการดัดแปลงหรือถูกทำลายโดยไม่เหมาะสม รวมถึงการทำให้มั่นใจว่าข้อมูลมีความถูกต้อง
3. **ความพร้อมใช้งานของข้อมูล (Availability)** คือ การทำให้มั่นใจว่า สามารถเข้าถึงข้อมูลและใช้งานได้อย่างทันเวลาและเชื่อถือได้

องค์กรมีความจำเป็นที่ต้องจัดให้มีการบริหารความเสี่ยงอย่างเหมาะสม จากการจำแนกข้อมูลตามความเสี่ยงและผลกระทบ โดยการกำหนดระดับความเสี่ยงของข้อมูลส่วนบุคคลในชุดต่าง ๆ (Data Risk Level) และผลกระทบที่อาจเกิดขึ้น (Impact) กับองค์กรหรือบุคคลหากถูกละเมิดความปลอดภัย สามารถแบ่งได้เป็น 3 ระดับ ได้แก่

1. **ผลกระทบระดับต่ำ (Low)** คือ มีแนวโน้มที่จะมีผลกระทบอย่างจำกัด (Limited Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น
    1. ทำให้ความสามารถในการปฏิบัติภารกิจลดลงในขอบเขตและระยะเวลาที่องค์กรสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิภาพระบบสารสนเทศลดลงอย่างสังเกตเห็นได้
    2. ส่งผลให้เกิดความเสียหายเล็กน้อยต่อทรัพย์สินขององค์กร
    3. ความเสียหายทางการเงินเล็กน้อย
    4. ส่งผลให้เกิดอันตรายต่อบุคคลอย่างเล็กน้อย
2. **ผลกระทบระดับกลาง (Moderate)** มีแนวโน้มที่จะมีผลกระทบอย่างมาก (Serious Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

1. ทำให้เกิดการลดลงอย่างมีนัยสำคัญในความสามารถในการปฏิบัติภารกิจในระดับและระยะเวลาที่องค์กรสามารถปฏิบัติหน้าที่หลักได้ แต่ประสิทธิภาพของระบบสารสนเทศจะลดลงอย่างมีนัยสำคัญ
2. ส่งผลให้เกิดความเสียหายอย่างมีนัยสำคัญต่อทรัพย์สินขององค์กร
3. ส่งผลให้เกิดการสูญเสียทางการเงินอย่างมีนัยสำคัญ
4. ส่งผลให้เกิดอันตรายอย่างมีนัยสำคัญต่อบุคคล แต่ไม่ถึงกับการสูญเสียชีวิตหรือได้รับบาดเจ็บร้ายแรงถึงชีวิต

3. **ผลกระทบระดับสูง (High)** มีแนวโน้มที่จะมีผลกระทบอย่างร้ายแรงหรือหายนะ (Severe or Catastrophic Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล เช่น
   1. ทำให้เกิดความเสื่อมโทรมอย่างรุนแรงในหรือสูญเสียความสามารถในการปฏิบัติภารกิจในขอบเขตและระยะเวลาที่องค์กรไม่สามารถปฏิบัติหน้าที่หลักอย่างน้อยหนึ่งอย่าง
   2. ส่งผลให้เกิดความเสียหายอย่างใหญ่หลวงต่อทรัพย์สินขององค์กร
   3. ส่งผลให้เกิดการสูญเสียทางการเงินที่สำคัญ
   4. ส่งผลให้เกิดอันตรายอย่างรุนแรงต่อความปลอดภัยของชีวิตหรือได้รับบาดเจ็บร้ายแรงถึงชีวิต

การจำแนกข้อมูลสามารถกำหนดระดับการจำแนกข้อมูลได้หลากหลายระดับ ขึ้นอยู่กับความเหมาะสมขององค์กร ดังตารางด้านล่างเป็นตัวอย่างการจำแนกข้อมูลออกเป็น 5 ระดับ (ระดับ 0 ถึง 4) ซึ่งกำหนดให้ PII หรือ ข้อมูลส่วนบุคคลอยู่ในระดับ 3 “Confidential” ซึ่งเป็นข้อมูลที่ถูกจัดให้ได้รับการคุ้มครองตามกฎหมาย ดังนั้นองค์กรจึงต้องจัดให้มีมาตรการการรักษาความปลอดภัยของข้อมูลดังกล่าวให้เหมาะสมกับความเสี่ยง

Level of Dataset	Data Classification	Refer to
Level 0	Open	หมายถึงข้อมูลที่ไม่จัดอยู่ในกลุ่ม 1,2,3 หรือ 4 เป็นข้อมูลที่พร้อมให้สาธารณชนเข้าถึงได้บนเว็บไซต์ หรือเป็นชุดข้อมูลที่รัฐเปิดเผย
Level 1	Public Not Proactively Released	หมายถึง ข้อมูลที่ไม่ได้รับการคุ้มครองจากการเปิดเผยต่อสาธารณะหรือถูกควบคุมภายใต้กฎหมายข้อบังคับหรือสัญญาใด ๆ เป็นข้อมูลที่ถูกเผยแพร่บนอินเทอร์เน็ตหรือสาธารณะ มีแนวโน้มที่จะเสี่ยงต่อความปลอดภัย ความเป็นส่วนตัวหรือความปลอดภัยของแต่ละบุคคลที่ถูกระบุไว้ในชุดข้อมูล

Level 2	For District Government Use	หมายถึง ข้อมูลสำหรับการใช้งานของรัฐ ข้อมูลที่ไม่ใช่ข้อมูลอ่อนไหว และอาจมีการเผยแพร่ภายในรัฐบาล ไม่มีข้อจำกัดตามกฎหมาย ข้อบังคับตามสัญญา เป็นข้อมูลการดำเนินธุรกิจของภาครัฐเป็นหลัก
Level 3	Confidential	หมายถึงข้อมูลที่เป็นความลับ เป็นข้อมูลที่ได้รับการป้องกันการเปิดเผยตามกฎหมาย ข้อบังคับ หรือสัญญา ซึ่งเป็นข้อมูลที่มีความอ่อนไหวหรือได้รับการคุ้มครองอย่างถูกต้องตามกฎหมาย กฎระเบียบหรือข้อบังคับตามสัญญาจากการเปิดเผยต่อหน่วยงานสาธารณะอื่น ๆ ซึ่งข้อมูลที่ถูกจำแนกอยู่ในประเภทนี้ นั้นรวมถึง ข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัว เช่น ข้อมูลที่ทำให้ระบุตัวบุคคลได้ ข้อมูลอ่อนไหว เป็นต้น
Level 4	Restricted Confidential	หมายถึงข้อมูลความลับที่ถูกจำกัด คือข้อมูลที่หากถูกเปิดเผยโดยไม่ได้รับอนุญาตอาจทำให้เกิดความเสียหายร้ายแรง อาจส่งผลต่อความปลอดภัยของชีวิตหรือการได้รับบาดเจ็บร้ายแรงถึงชีวิตต่อผู้ที่ถูกระบุไว้ในชุดข้อมูล ส่งผลที่ลดลงอย่างมีนัยสำคัญในความสามารถในการปฏิบัติภารกิจในระดับและระยะเวลาที่องค์กรสามารถปฏิบัติหน้าที่หลักได้

ตารางด้านล่าง แสดงความสัมพันธ์ของผลกระทบที่อาจเกิดขึ้นหากถูกละเมิดในแต่ละวัตถุประสงค์ด้านความปลอดภัย (Potential Impact Definitions for Security Objectives)

ผลกระทบที่อาจเกิดขึ้น (Potential Impact)			
Security Objective	**Low**	**Moderate**	**High**
"Confidentiality" การจำกัดการเข้าถึงและการเปิดเผยข้อมูล รวมถึงวิธีการปกป้องความเป็นส่วนตัวและสิทธิในข้อมูล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างจำกัด ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างมาก ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต คาดว่าอาจจะมีผลกระทบในทางลบอย่างร้ายแรงต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล
"Integrity" การรักษาความปลอดภัยของข้อมูล จากการดัดแปลงหรือถูก	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าอาจจะมีผลกระทบอย่างจำกัดต่อการดำเนินงานของ	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าอาจจะมีผลกระทบอย่างมาก ต่อการดำเนินงาน	การดัดแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตคาดว่าอาจจะมีผลกระทบอย่างร้ายแรงต่อการดำเนินงานของ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ทำลายโดยไม่เหมาะสม รวมถึงการทำให้มั่นใจว่าข้อมูลมีความถูกต้อง	องค์กร ทรัพย์สินขององค์กรหรือบุคคล	ขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	องค์กร ทรัพย์สินขององค์กรหรือบุคคล
"Availability" การทำให้มั่นใจว่าสามารถเข้าถึงข้อมูลและใช้งานได้อย่างทันเวลาและเชื่อถือได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่าอาจมีผลกระทบอย่างจำกัดต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่าอาจมีผลกระทบอย่างมาก ต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศของข้อมูล คาดว่าอาจมีผลกระทบอย่างร้ายแรงต่อการดำเนินงานขององค์กร ทรัพย์สินขององค์กรหรือบุคคล

3.2.3 ปัจจัยในการกำหนดผลกระทบที่อาจเกิดขึ้นต่อการรักษาความลับของข้อมูลส่วนบุคคล (Factors for Determining PII Confidentiality Impact Levels)

ในการพิจารณาถึงผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดของข้อมูลส่วนบุคคล ธนาคารควรทำการประเมินความเสี่ยงจากปัจจัยที่สำคัญดังที่จะกล่าวต่อไปนี้ ซึ่งในกระบวนการพิจารณาปัจจัยต่าง ๆ ธนาคารควรจะต้องพิจารณาปัจจัยที่เกี่ยวข้องร่วมกัน เนื่องจากการพิจารณาเพียงปัจจัยเดียวนั้นอาจให้ผลลัพธ์ของผลกระทบที่อาจเกิดขึ้น (Potential Impact) ในระดับต่ำ แต่ปัจจัยประการอื่นอาจบ่งชี้ได้ว่าผลกระทบที่อาจเกิดขึ้นอยู่ในระดับสูงได้ ซึ่งผลลัพธ์นั้นควรแทนที่ปัจจัยแรก

ในขั้นตอนการพิจารณาปัจจัยที่อาจส่งผลกระทบต่อการรักษาความลับของข้อมูลส่วนบุคคล จะช่วยให้ธนาคารสามารถกำหนดการรักษาความปลอดภัยของข้อมูลได้ดีและเหมาะสมกับความเสี่ยงยิ่งขึ้น ซึ่งจะช่วยให้ธนาคารเข้าใจถึงกระบวนการ และเพื่อช่วยใช้ในการประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคล

Factors for Determining PII Confidentiality Impact Levels
Identifiability
Quantity of PII
Data Field Sensitivity
Context of Use
Access to and Location of PII

1. (Identifiability) ความสามารถในการระบุตัวบุคคล: ธนาคารจะต้องพิจารณาว่าข้อมูลส่วนบุคคลดังกล่าว มีความสามารถในการระบุตัวบุคคลได้มากน้อยเพียงใด เช่น ชุดข้อมูลที่มี ชื่อนามสกุล หมายเลขโทรศัพท์และที่อยู่อีเมลนั้นสามารถระบุตัวบุคคลได้โดยตรง ชุดข้อมูลที่อาจระบุตัวตนได้โดยอ้อมอาจต้องพิจารณาเพิ่มเติมถึงความสามารถในการระบุตัวบุคคลตาม 3 ลักษณะ ได้แก่ ความสามารถในการแยกแยะ (Distinguishability) การติดตาม (Traceability) และการเชื่อมโยง (Linkability) ดังที่ได้กล่าวไว้ในหัวข้อการระบุข้อมูลส่วนบุคคล (Identifying Personal Identifiable Information)

2. (Quantity of PII) ปริมาณของข้อมูลส่วนบุคคล: ธนาคารจะต้องทำการประเมินว่า ข้อมูลส่วนบุคคลที่ธนาคารมีอยู่นั้นมีปริมาณมากน้อยเพียงใด การถูกละเมิดข้อมูลส่วนบุคคลที่มีจำนวนน้อยกับที่มีจำนวนมากย่อมก่อให้เกิดผลกระทบต่างกัน ไม่เพียงแต่ผลกระทบแก่เจ้าของข้อมูลส่วนบุคคล แต่รวมถึงผลกระทบต่อชื่อเสียงของธนาคารเองด้วย รวมถึงค่าใช้จ่ายในที่ธนาคารจะต้องทำการแก้ไขสาเหตุการละเมิดหรือค่าใช้จ่ายที่ต้องรับผิดชอบให้กับเจ้าของข้อมูลส่วนบุคคล หรือค่าปรับตามกฎหมาย ดังนั้นธนาคารอาจพิจารณาให้ผลกระทบที่อาจเกิดขึ้นอยู่ในระดับสูงสำหรับชุดข้อมูลขนาดใหญ่ แต่ก็ไม่ได้หมายความว่าถ้ามีชุดข้อมูลขนาดเล็กแล้วจะมีระดับความเสี่ยงที่ต่ำจึงต้องพิจารณาปัจจัยอื่นด้วย

3. (Data Field Sensitivity) ความอ่อนไหวของข้อมูล: ธนาคารควรประเมินความอ่อนไหวของข้อมูลส่วนบุคคลที่ธนาคารทำการเก็บรวบรวม ตัวอย่างเช่น ข้อมูลทางการเงิน ข้อมูลเลขบัตรประจำตัวประชาชน ข้อมูลสุขภาพ ย่อมมีความอ่อนไหวมากกว่า ข้อมูลหมายเลขโทรศัพท์ หรือรหัสไปรษณีย์ ของเจ้าของข้อมูลส่วนบุคคล ดังนั้นธนาคารจะต้องกำหนดระดับผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดข้อมูลสำหรับข้อมูลที่มีความอ่อนไหวอยู่ในระดับที่สูงกว่าข้อมูลที่มีความอ่อนไหวน้อยกว่า ซึ่งธนาคารควรกำหนดให้ข้อมูลอ่อนไหวอยู่ในระดับความเสี่ยงปานกลางเป็นอย่างน้อย อย่างไรก็ตามธนาคารต้องคำนึงถึงบริบทในการใช้งานด้วย เช่น ข้อมูลเขตที่อยู่ รหัสไปรษณีย์ สถานที่เกิด อาจมีความอ่อนไหวมากขึ้นหากถูกนำไปใช้นอกเหนือจากวัตถุประสงค์เดิม เช่นถูกนำไปใช้ในการยืนยันตัวตนในการกู้รหัสผ่านของเจ้าของข้อมูลส่วนบุคคล

4. (Context of Use) บริบทในการใช้ข้อมูล: เป็นปัจจัยที่เกี่ยวข้องกับการใช้ข้อมูลอย่าง ถูกต้อง เป็นธรรม และโปร่งใส บริบทในการใช้ข้อมูลสามารถพิจารณาได้จากวัตถุประสงค์ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล เช่น การเก็บรวบรวมข้อมูลเพื่อใช้ในการวิเคราะห์เชิงสถิติ เพื่อประโยชน์ตามกฎหมาย เพื่อการคำนวณภาษี เป็นต้น ซึ่งการประเมินบริบทของการใช้ข้อมูล จะช่วยให้ธนาคารประเมินระดับของผลกระทบที่อาจเกิดขึ้นกับบุคคลหรือธนาคารจากการเปิดเผยข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5. (Access to and Location of PII) การเข้าถึงและที่เก็บข้อมูล: ธนาคารอาจพิจารณาถึงความจำเป็นในการใช้ข้อมูลส่วนบุคคลเพื่อบรรลุวัตถุประสงค์ เพื่อใช้ในการกำหนดความจำเป็นในการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลได้อย่างเหมาะสม เนื่องจากหากข้อมูลส่วนบุคคลถูกเข้าถึงบ่อยครั้งหรือเข้าถึงได้ด้วยบุคคลจำนวนมาก จะเป็นการเพิ่มโอกาสที่ข้อมูลอาจรั่วไหลมากขึ้น รวมถึงหากข้อมูลสามารถเข้าถึงได้จาก เครื่องมือ หรือระบบอื่น ๆ หรือส่วนงานต่าง ๆ เช่น การเข้าระบบผ่านทางเว็บไซต์ หรือผ่านทาง Application ทั้งจากภายในธนาคารและภายนอกธนาคาร ย่อมทำให้ความเสี่ยงในการรั่วไหลมากขึ้น ซึ่งธนาคารอาจกำหนดให้ระดับของผลกระทบที่อาจเกิดขึ้นสูงได้

4. หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

แนวปฏิบัติฉบับนี้อ้างอิงถึงหลักการตาม GDPR Article 5 (“Principles Relating to Processing of Personal Data”) สาระสำคัญกล่าวถึงหลักการทั้ง 7 อย่างในการประมวลผลข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นสิ่งที่พึงระลึกก่อนทำการประมวลผลข้อมูลส่วนบุคคล ธนาคารควรทำความเข้าใจหลักการที่สำคัญเหล่านี้ จะช่วยให้เข้าใจถึงหลักการและข้อจำกัดในการประมวลข้อมูลส่วนบุคคล เพื่อที่จะสามารถพิจารณาความเหมาะสมในการประมวลผลข้อมูลในกรณีอื่นได้ และหลักการเหล่านี้จะถูกอ้างอิงในการตีความของเนื้อหาส่วนอื่นในเอกสารแนวปฏิบัติ ที่จะต้องมีความสอดคล้องกับหลักการสำคัญทั้ง 7 นี้

4.1 Principle 1 : ("Lawfulness, Fairness, and Transparency”)

ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลโดยชอบด้วยกฎหมาย มีความเป็นธรรมและโปร่งใส

- “Lawfulness” หมายถึงในการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องสามารถระบุ “ฐานทางกฎหมาย” (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคลธนาคารจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง และจะต้องมีความระมัดระวังมากขึ้นในการประมวลผลข้อมูลอ่อนไหว (Sensitive Personal Data) ซึ่งถ้าหากผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถระบุฐานทางกฎหมายในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ จะเป็นการขัดต่อหลักการข้อนี้ รวมทั้งอาจเป็นการขัดต่อกฎหมาย ซึ่งเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุถึงเจ้าของข้อมูลส่วนบุคคลได้
- “Fairness” หมายถึงความเป็นธรรม ในการประมวลผลข้อมูลส่วนบุคคลจะต้องทำในลักษณะที่สมเหตุสมผลตามความคาดหมายของเจ้าของข้อมูลส่วนบุคคล มีความยุติธรรมและไม่เป็นการละเมิดสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

- "Transparency" หมายถึงความโปร่งใส โดยทั่วไปแล้วความโปร่งใสนั้นเชื่อมโยงกับความเป็นธรรม เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอย่างโปร่งใส ผู้ควบคุมข้อมูลจะต้องแสดงรายละเอียดในการประมวลผลข้อมูลโดยชัดเจน เพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจถึงการประมวลผลข้อมูลของตนได้ ตัวอย่างเช่น เริ่มต้นจากผู้เก็บรวบรวมข้อมูลส่วนบุคคลแสดงตนว่าใครคือผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีการประมวลผลข้อมูลส่วนบุคคลอย่างไร รวมทั้งสามารถเปิดเผยให้แก่เจ้าของข้อมูลส่วนบุคคลทราบและตรวจสอบได้ นอกจากนั้นควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบด้วยภาษาที่ง่ายต่อความเข้าใจ ไม่ซับซ้อนหรือไม่ทำเกิดความเข้าใจผิดได้ง่าย

4.2 Principle 2 : ("Purpose Limitation")

การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องเก็บเฉพาะที่เกี่ยวข้อง จำเป็น เพื่อประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อันชอบด้วยกฎหมายที่ระบุไว้อย่างชัดเจน และชอบธรรม อีกทั้งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่นำไปประมวลผลต่อในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้นและไม่สามารถนำไปใช้กับวัตถุประสงค์ใหม่ที่นอกเหนือจากวัตถุประสงค์ในการเก็บรวบรวมที่ระบุไว้ในตอนแรก สำหรับการใช้ข้อมูลในบริบทนี้ หมายความรวมถึง การใช้ เปิดเผย และการโอนข้อมูลส่วนบุคคลด้วย

ตัวอย่าง 1 การประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการส่งเสริมการขายและการประชาสัมพันธ์เกี่ยวกับผลิตภัณฑ์และบริการต่างๆ ธนาคารอาจทำการเก็บรวบรวมข้อมูลชื่อ นามสกุล อีเมลและหมายเลขโทรศัพท์ของลูกค้า ซึ่งเป็นการเก็บรวบรวมและใช้ข้อมูลเฉพาะเท่าที่จำเป็นในการประมวลผลข้อมูลตามวัตถุประสงค์ดังกล่าว

ตัวอย่าง 2 ธนาคารไม่สามารถประมวลผลตามวัตถุประสงค์ที่นอกเหนือจากวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยตามที่ระบุไว้ในตอนแรก เช่น ปัจจุบันธนาคารประมวผลข้อมูลส่วนบุคคลของลูกค้า เพื่อวัตถุประสงค์ในการให้สินเชื่อ ภายหลังธนาคารต้องการจะเปิดเผยข้อมูลส่วนบุคคลของลูกค้าให้กับบริษัทประกันภัย เพื่อวัตถุประสงค์ในการขายผลิตภัณฑ์อื่น ธนาคารไม่สามารถเปิดเผยข้อมูลส่วนบุคคลให้บริษัทประกันภัยได้ เนื่องจากวัตถุประสงค์นั้นเป็นวัตถุประสงค์อื่นที่นอกเหนือจากวัตถุประสงค์เดิมที่ใช้ในการประมวลผลข้อมูล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

4.3 Principle 3 : (“Data Minimisation”)

ในการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่กระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย รวมถึงระยะเวลาในการเก็บ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะดำเนินการเท่าที่จำเป็น เกี่ยวข้อง และจำกัดตามวัตถุประสงค์ในการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลทราบ

ตัวอย่าง 1 ในการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้า ธนาคารจะต้องทำการเก็บเท่าที่จำเป็นเพื่อใช้ในการประมวลผลข้อมูลตามวัตถุประสงค์ที่แจ้งต่อลูกค้า ธนาคารควรที่จะพิจารณาอย่างรอบคอบว่า ข้อมูลใดมีความจำเป็นที่ต้องทำการเก็บรวบรวม เช่น ในการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อเปิดบัญชีออมทรัพย์กับธนาคาร จะต้องทำการขอข้อมูลชื่อ นามสกุล ที่อยู่ และข้อมูลในการติดต่อลูกค้า ซึ่งมีความจำเป็นที่จะต้องทำการเก็บข้อมูลเหล่านี้ เพื่อใช้ในการให้บริการทางการเงินแก่ลูกค้า ซึ่งธนาคารไม่ควรทำการเก็บรวบรวม เชื้อชาติ ศาสนา เนื่องจากข้อมูลดังกล่าว เกินความจำเป็นในการประมวลผลข้อมูลตามวัตถุประสงค์ในการเปิดบัญชีออมทรัพย์

ตัวอย่าง 2 กรณีที่ลูกค้าขอสินเชื่อกับธนาคาร ธนาคารมีความจำเป็นที่จะต้องทำการเก็บรวบรวมข้อมูลคู่สมรสเพื่อใช้ในการพิจารณาการให้สินเชื่อ ดังนั้นธนาคารสามารถเก็บรวบรวมข้อมูลผู้สมรสได้เนื่องจากมีความจำเป็นในการพิจารณาการให้บริการของธนาคาร

4.4 Principle 4 : (“Accuracy”)

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบหรือแก้ไขโดยไม่ล่าช้า

ตัวอย่าง ในขั้นตอนการเก็บรวบรวมข้อมูลส่วนบุคคล ธนาคารจะต้องทำการตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลตามข้อกำหนดหรือกฎหมาย ภายหลังหากลูกค้าพบว่าข้อมูลไม่ถูกต้องหรือประสงค์จะแก้ไขข้อมูล ธนาคารจะต้องดำเนินการแก้ไขตามที่ลูกค้าประสงค์จะแก้ไขโดยไม่ล่าช้าเพื่อให้ข้อมูลถูกต้องสมบูรณ์และเป็นปัจจุบันที่สุด ดังนั้นธนาคารจึงควรจัดให้มีช่องทางการติดต่อที่ง่าย สะดวก รวดเร็ว เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการได้โดยง่าย

4.5 Principle 5 : (“Storage Limitation”)

ข้อมูลส่วนบุคคลจะต้องไม่เก็บเกินความจำเป็นตามระยะเวลาที่เหมาะสมเพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือเก็บตามระยะเวลาที่กฎหมายกำหนด

ตัวอย่าง ธนาคารทำการเก็บข้อมูลเกี่ยวกับสินเชื่อ เป็นระยะเวลา 10 ปี หลังชำระหนี้เสร็จสิ้น เนื่องจากสอดคล้องตามอายุความและสอดคล้องตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

4.6 Principle 6 : (“Integrity and Confidentiality”)

ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการที่ทำให้มั่นใจว่ามีการรักษาความปลอดภัยของข้อมูลส่วนบุคคล และข้อมูลส่วนมีความสมบูรณ์ถูกต้อง โดยจัดให้มีมาตรการทั้งในเชิงบริหารจัดการและเชิงเทคนิคที่มีความเหมาะสม และมีการป้องกันการประมวลผลจากบุคคลที่ไม่ได้รับอนุญาตหรือการประมวลผลอันมิชอบด้วยกฎหมาย มีการป้องกันการสูญหาย เสียหาย หรือการถูกทำลาย โดยไม่ได้ตั้งใจ

ตัวอย่าง 1 ธนาคารมีระบบฐานข้อมูลที่เกี่ยวข้องกับการขออนุมัติสินเชื่อ ซึ่งพนักงานแผนกสินเชื่อจะสามารถเข้าถึงฐานข้อมูลดังกล่าว เพื่อใช้ในการหาข้อมูลของลูกค้าเพื่อนำไปวิเคราะห์การให้สินเชื่อของธนาคารได้ เช่น การค้นหาข้อมูลสินทรัพย์และหนี้สินของลูกค้า เป็นต้น อย่างไรก็ตามพนักงานแผนกอื่นที่ไม่ได้ทำหน้าที่เกี่ยวข้องกับการวิเคราะห์สินเชื่อ ไม่ควรที่จะสามารถเข้าถึงฐานข้อมูลดังกล่าวได้ ตามหลัก Confidentiality ตัวอย่าง 2 ธนาคารมีระบบการจัดการที่เกี่ยวกับการขออนุมัติสินเชื่อ ซึ่งผู้วิเคราะห์สินเชื่อจะสามารถบันทึกข้อมูลคำสั่งการขอสินเชื่อและข้อมูลเครดิตต่าง ๆ เพื่อประกอบการพิจารณาการให้สินเชื่อแก่ลูกค้า และทำการส่งคำขออนุมัติไปยังผู้พิจารณาเครดิต อย่างไรก็ตามผู้พิจารณาเครดิตจะสามารถทำการอนุมัติหรือปฏิเสธการให้สินเชื่อผ่านระบบดังกล่าวได้ แต่จะไม่สามารถทำการแก้ไขข้อมูลเครดิตที่ผู้วิเคราะห์สินเชื่อทำการบันทึกไว้ได้ รวมทั้งพนักงานแผนกอื่นก็ไม่สามารถทำการเข้าถึงและแก้ไขได้เช่นกัน ตามหลัก Integrity นั่นคือข้อมูลจะต้องคงความถูกต้องสมบูรณ์ ไม่ถูกเปลี่ยนแปลง แก้ไข หรือลบได้ เว้นแต่ผู้ที่ได้รับสิทธิอย่างถูกต้องและเหมาะสมเท่านั้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

4.7 Principle 7 : (“Accountability”)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่และความรับผิดชอบในการประมวลผลข้อมูลให้เป็นไปตามหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

ตัวอย่าง 1 ธนาคารมีการเก็บข้อมูลส่วนบุคคลของลูกค้า ไว้ในระบบฐานข้อมูลของธนาคาร (Database) และมีการเก็บข้อมูลในเครื่องคอมพิวเตอร์ รวมถึงที่เก็บข้อมูลแบบพกพา ซึ่งในการเก็บข้อมูลทั้งหมดนี้ ธนาคารมีหน้าที่และความรับผิดชอบ (“Accountability”) ในการจัดให้มีมาตรการรักษาความมั่นคงและปลอดภัยของข้อมูล และมีจัดให้มีการควบคุมการเข้าถึงข้อมูลตามหลัก Integrity and Confidentiality

ตัวอย่าง 2 ธนาคารมีการจัดจ้างบริษัทภายนอก เพื่อทำแคมเปญการตลาด (Marketing Campaign) ในการทำแคมเปญให้ตรงกับความต้องการของลูกค้านั้น ธนาคารมีความจำเป็นที่จะต้องเปิดเผยข้อมูลลูกค้าบางรายเฉพาะกลุ่มลูกค้าเป้าหมาย และเปิดเผยเฉพาะข้อมูลที่จำเป็นที่ใช้ในการประมวลผลตามวัตถุประสงค์ (“Data Minimisation”) เพื่อให้บริษัท Marketing ทำการสำรวจความคิดเห็นของลูกค้า ตามวัตถุประสงค์ที่ได้แจ้งและได้ทำการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ("Lawfulness, Fairness, and Transparency”) ซึ่งธนาคารไม่สามารถเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่ได้แจ้งไว้ได้ (“Purpose Limitation”) ในกรณีนี้ธนาคารจะต้องมีการดำเนินการเพื่อให้มั่นใจว่าข้อมูลที่ส่งไปนั้นมีการจัดการอย่างเหมาะสม มีการรักษาความปลอดภัยของข้อมูล (“Integrity and Confidentaility”) และต้องดำเนินการให้ลบข้อมูลออกทั้งหมดหลังจากที่บริษัท Marketing ทำงานให้กับธนาคารเสร็จเรียบร้อยแล้ว (“Storage Limitation”) เนื่องจากหมดความจำเป็นในการเก็บรักษาและเพื่อป้องกันการรั่วไหล หรือการถูกนำไปใช้หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ตามตัวอย่างที่ได้กล่าวมานี้ ธนาคารมีหน้าที่ในการประมวลผลข้อมูลภายใต้หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (“Accountability”)

5. การเก็บรวบรวมข้อมูลส่วนบุคคล

5.1 วัตถุประสงค์ในการเก็บรวบรวมข้อมูล

5.1.1 ธนาคารจะต้องทำการแจ้งให้แก่เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ว่าข้อมูลส่วนบุคคลของลูกค้าจะถูกนำไปใช้อย่างไรเพื่อวัตถุประสงค์ใด อีกทั้งความจำเป็นที่ต้องใช้ข้อมูลเหล่านี้ ในกรณีที่มีความจำเป็นที่จะต้องเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลภายนอก ก็ต้องสามารถระบุวัตถุประสงค์ได้ว่าเพื่อวัตถุประสงค์อะไรรวมทั้งประเภทของบุคคลหรือหน่วยงานที่ข้อมูล

อาจถูกเปิดเผย ซึ่งธนาคารจะต้องทำการดำเนินการแจ้งลูกค้าผ่านช่องทางและวิธีการที่เหมาะสม เช่น ประกาศความเป็นส่วนตัวหรือนโยบายความเป็นส่วนตัว ผ่านทางเว็บไซต์ของธนาคาร เป็นต้น

5.1.2 ในการระบุวัตถุประสงค์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ธนาคารไม่จำเป็นต้องระบุถึงขั้นตอนหรือกระบวนการปฏิบัติงานทุก ๆ กิจกรรม แต่ให้ระบุถึงวัตถุประสงค์ที่เกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคล เหตุผลที่เกี่ยวข้องหรือประโยชน์อันใดที่เกี่ยวข้อง รวมถึงฐานในการประมวลผลข้อมูล หากลูกค้ามีข้อสงสัยในการเก็บรวบรวมข้อมูล ใช้ เปิดเผย ธนาคารต้องจัดให้มีช่องทางในการร้องขอหรือจัดให้มีข้อมูลติดต่อธนาคารอย่างชัดเจนไปยัง DPO หรือบุคคลที่ธนาคารกำหนดให้ทำหน้าที่ในการรับเรื่อง เพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิร้องขอได้

5.1.3 ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ธนาคารต้องกระทำเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย ตามหลักการ Principle 1 : ("Lawfulness, Fairness, and Transparency"), Principle 2 : ("Purpose Limitation") และ Principle 3 : ("Data Minimisation") ซึ่งในแต่ละกิจกรรมการประมวลผลข้อมูล ธนาคารจะต้องสามารถระบุ "ฐานทางกฎหมาย" (Lawful Basis) ที่เหมาะสมในการประมวลผลให้ได้ฐานใดฐานหนึ่ง

5.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย ธนาคารจะต้องสามารถระบุฐานในการประมวลผลตามกฎหมาย (Lawful basis) ในแต่ละกิจกรรมการประมวลผลข้อมูลให้ได้ฐานใดฐานหนึ่ง ตามที่จะกล่าวดังต่อไปนี้และจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงฐานในการประมวลผลข้อมูล รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลและข้อจำกัดในแต่ละฐานที่แตกต่างกันด้วย

5.2.1 ฐานความยินยอม (Consent)

ธนาคารสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลได้ใน กรณีที่เจ้าของข้อมูลส่วนบุคคลสมัครใจ และให้ความยินยอมอย่างชัดแจ้ง (Explicit Consent) ที่จะให้ทำการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม ฐานความยินยอมเหมาะสมเมื่อต้องการขอความยินยอมเพื่อประมวลผลข้อมูลส่วนบุคคลในเรื่องที่ไม่จำเป็นในการปฏิบัติตามสัญญาและไม่สามารถอ้างฐานอื่นใดในการประมวลผลข้อมูลทางกฎหมายได้ นอกจากนั้นการให้ความยินยอม จะต้องเป็นสิ่งที่ให้เจ้าของข้อมูลส่วนบุคคลทำการเลือกว่าจะให้หรือปฏิเสธได้และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา สำหรับเงื่อนไขและรายละเอียดการขอ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ความยินยอมภายใต้ฐานความยินยอมโปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “5.3 ความยินยอม (Consent)”

5.2.2 ฐานสัญญา (Contract)

ธนาคารสามารถใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล หรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนที่จะเข้าสู่การทำสัญญา หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ไม่สามารถใช้ฐานสัญญาในการประมวลผลข้อมูลอ่อนไหว (Sensitive Personal Data) สำหรับรายละเอียดและเงื่อนไขในการประมวลผลข้อมูลอ่อนไหวโปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “5.4 ข้อมูลอ่อนไหว (Sensitive Personal Data)”

กรณีที่ธนาคารมีความจำเป็นที่จะต้องเปิดเผยข้อมูลของลูกค้าไปยังบุคคลที่สาม หากการเปิดเผยนั้นไม่ใช่เพื่อวัตถุประสงค์ทางการตลาด สำหรับกรณีนี้หากลูกค้าไม่ให้ความยินยอมจะกระทบต่อการดำเนินงานของธนาคารอย่างมีนัยสำคัญ หรือไม่สามารถให้บริการอย่างเป็นธรรมและต่อเนื่องได้ เช่น การเปิดเผยข้อมูลแก่ผู้ให้บริการภายนอก หรือตัวแทนของผู้ให้บริการ หรือผู้รับจ้างช่วงงานต่อ เพื่อสนับสนุนการให้บริการของผู้ให้บริการ การเปิดเผยข้อมูลให้หน่วยงานราชการตามกฎหมาย และการเปิดเผยข้อมูลให้กับบริษัทพันธมิตรในลักษณะ Co-brand เป็นต้น ธนาคารสามารถกำหนดให้การเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สามดังกล่าวเป็นส่วนหนึ่งของเงื่อนไขในการขอใช้บริการได้ ตามข้อกำหนดของประกาศธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct) และการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลที่สามนี้ ถือเป็นการกระทำภายใต้ฐานสัญญาที่ทำกับลูกค้า

ตัวอย่าง 1 ลูกค้าขอรับบริการจากธนาคาร เช่น ขอสินเชื่อ เปิดบัญชีเงินฝากออมทรัพย์หรือกระแสรายวัน การทำบัตรเครดิต รวมทั้งการขอรับบริการอิเล็กทรอนิกส์ต่าง ๆ อันได้แก่ Mobile Banking Application และ Internet Banking ธนาคารควรใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บริการแก่ลูกค้าตามข้อกำหนดและเงื่อนไขการให้บริการ ที่ลูกค้าได้ตกลงตามข้อผูกพันดังกล่าว

ตัวอย่าง 2 ธนาคารทำการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าไปยังบุคคลที่สาม (Outsource) ที่รับจ้างการจัดสัมมนา (Organizer) เพื่อดูแลความเรียบร้อยภายในงานและประสานงานต่างๆ ในกรณีนี้ธนาคารสามารถเปิดเผยข้อมูลภายใต้ฐานสัญญาได้ ซึ่งการเปิดเผยข้อมูลจะต้องอยู่ภายใต้เงื่อนไขของสัญญาที่ธนาคารทำไว้กับบริษัทรับจ้างการจัดสัมมนา

ตัวอย่างที่ 3 ในการให้สินเชื่อหรือการทวงถามชำระหนี้ ธนาคารมีความจำเป็นต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลที่เป็นข้อมูลทางการเงินของลูกค้า อันได้แก่ ข้อมูลที่เกี่ยวข้องในการใช้วิเคราะห์สินเชื่อ และข้อมูลการจ่ายชำระเพื่อใช้ในการติดตามหรือทวงถามหนี้ เช่น ข้อมูลการผิดนัดชำระของลูกหนี้ ข้อมูลการใช้เงินกู้ผิดวัตถุประสงค์ ข้อมูลบุคคลที่ถูกประกาศให้เป็นบุคคลล้มละลาย ข้อมูลที่ได้รับจากบริษัทข้อมูลเครดิต ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ภายใต้ฐานสัญญา

ตัวอย่างที่ 4 สำหรับ Mobile Banking Application กรณีลูกค้าเป็นการแสดง/ตั้งค่ารายการโปรดที่เป็นข้อมูลของลูกค้าถือเป็นการให้บริการตามฐานสัญญา

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5.2.3 ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

กรณีที่การประมวลผลข้อมูลจำเป็นต่อการปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น โดยเป็นการป้องกันอันตรายอันเกิดต่อสุขภาพและชีวิต ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ฐานการประมวลผลข้อมูลส่วนบุคคลนี้ได้ หากเจ้าของข้อมูลส่วนบุคคลอยู่ในสภาพที่ไม่สามารถให้ได้ความยินยอมได้ ทั่วไปใช้กับทางการแพทย์

ตัวอย่างที่ไม่ควรใช้ฐานประโยชน์สำคัญต่อชีวิต

ตัวอย่าง 1 ในกรณีที่ธนาคารทำการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงาน เช่น หมายเลขโทรศัพท์ของผู้ที่สามารถติดต่อได้ในกรณีฉุกเฉิน เพื่อใช้ติดต่อในกรณีฉุกเฉิน ซึ่งธนาคารสามารถทำการเก็บรวบรวมข้อมูลภายใต้ฐานสัญญาที่ทำระหว่างพนักงานและธนาคารในการรับเข้าทำงาน

ตัวอย่าง 2 ธนาคารต้องการเก็บรวบรวมข้อมูลที่เป็นข้อมูลอ่อนไหวของพนักงาน เช่น ข้อมูลกรุ๊ปเลือดของพนักงาน หรือข้อมูลเกี่ยวกับสุขภาพของพนักงาน เพื่อไว้ใช้ในกรณีฉุกเฉินหากเกิดอันตรายต่อชีวิตของพนักงาน ในกรณีนี้ข้อมูลที่ธนาคารต้องการเก็บรวบรวมเป็นข้อมูลอ่อนไหว หากก่อนหรือขณะทำการเก็บรวบรวมข้อมูลพนักงานอยู่ในสภาพที่สามารถให้ความยินยอมได้ ธนาคารสามารถเก็บรวบรวมข้อมูลดังกล่าวได้ภายใต้ฐานความยินยอมแต่ไม่สามารถอ้างฐานประโยชน์สำคัญต่อชีวิตได้เนื่องจาก จะใช้ได้เฉพาะกรณีที่เจ้าของข้อมูลส่วนบุคคลอยู่ในสภาพที่ไม่สามารถให้ได้ความยินยอมได้เท่านั้น

5.2.4 ฐานภารกิจของรัฐ (Public Task)

กรณีที่การประมวลผลเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบหมายให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยส่วนใหญ่ผู้ที่จะประมวลผลข้อมูลตามฐานนี้ได้มักเป็นเจ้าหน้าที่หรือองค์กรของภาครัฐ เช่น ศาล รัฐสภา หรือเจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติภารกิจตามกฎหมาย ซึ่งการประมวลผลโดยฐานดังกล่าวจะต้องสามารถอ้างอิงได้อย่างชัดเจนว่ากระทำภายใต้กฎหมายใดที่ให้อำนาจในการประมวลผลข้อมูล ซึ่งการใช้ฐานภารกิจของรัฐนั้นยังจำเป็นต้องมีการรักษาความปลอดภัยของข้อมูล เช่นเดียวกันกับฐานอื่น แต่เจ้าของข้อมูลส่วนบุคคลไม่สามารถ ใช้สิทธิในการ ลบ หรือโอนย้ายข้อมูลได้ แต่ยังมีสิทธิในการคัดค้านการประมวลผลได้

ตัวอย่าง 1 ธนาคารทำการเปิดเผยข้อมูลรายละเอียดสินเชื่อของลูกค้าให้กับกระทรวงการคลังสำหรับกลุ่มลูกค้าที่กู้ยืมเงินโครงการภาครัฐ เพื่อใช้ในการเบิกดอกเบี้ยที่กระทรวงการคลังสนับสนุนในบางส่วน ในกรณีนี้ธนาคารทำการเปิดเผยข้อมูลให้กับกระทรวงการคลังภายใต้ฐานการปฏิบัติตามกฎหมาย และกระทรวงการคลังทำการประมวลผลข้อมูลที่ได้รับจากธนาคารภายใต้ฐานภารกิจของรัฐ

ตัวอย่าง 2 ธนาคารมีหน้าที่ในการจัดทำการยื่นภาษีให้กับกรมสรรพากร ซึ่งกรมสรรพากรอาจขอให้ธนาคารเปิดเผยข้อมูลค่าใช้จ่ายเงินเดือนพนักงาน เพื่อทำการตรวจสอบความถูกต้องของข้อมูลในการคำนวณภาษีที่ธนาคารยื่นต่อกรมสรรพากร กรณีนี้ธนาคารสามารถเปิดเผยข้อมูลให้กับกรมสรรพากรภายใต้ฐานการปฏิบัติตามกฎหมาย และกรมสรรพากรทำการประมวลผลข้อมูลที่ได้รับจากธนาคารภายใต้ฐานภารกิจของรัฐ

5.2.5 ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

การใช้ฐานประโยชน์อันชอบธรรมเป็นหนึ่งในฐานกฎหมายที่มีความยืดหยุ่นมากที่สุดในการประมวลผลข้อมูลส่วนบุคคล แต่อย่างไรก็ตามฐานนี้ก็ไม่ได้เป็นฐานที่เหมาะสมที่สุดเสมอไป จะเหมาะสมเมื่อธนาคารประมวลผลข้อมูลส่วนบุคคลในแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้อย่างสมเหตุสมผล อีกทั้งมีผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลเพียงเล็กน้อย หรือในกรณีที่ธนาคารมีเหตุผลในการประมวลผลข้อมูลอย่างสมเหตุสมผลซึ่งธนาคารเองจะต้องอธิบายได้ หากธนาคารเลือกที่จะประมวลผลภายใต้ฐานประโยชน์อันชอบธรรม ธนาคารจะมีหน้าที่และความรับผิดชอบเพิ่มขึ้น ในการใช้ดุลพินิจอย่างมากในการประมวลผลข้อมูลส่วนบุคคล และการคุ้มครองสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เนื่องจากธนาคารจะต้องคำนึงถึงประโยชน์ของ 2 ฝั่ง อันได้แก่ผลประโยชน์อันชอบธรรมของธนาคารเองกับสิทธิและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ซึ่งการได้ประโยชน์อันชอบธรรมดังกล่าวจะต้องไม่เป็นการละเมิดหรือกระทบต่อสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งกับผู้เยาว์

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

1. Identify a legitimate interest		
What is purpose of data processing?	Necessary to meet the purposes of the data controller	Necessary for the purpose of third party's interest

2. Necessity test	
Important?	No other way?

3. Balancing test		
Expectation of others	Value-added?	Negative impact?

ตารางแสดงการประเมินการใช้ฐานผลประโยชน์อันชอบธรรม

Legitimate interest Assessment (LIA)

ในการประเมินการใช้ฐานผลประโยชน์อันชอบธรรม สามารถทำได้โดยพิจารณา 3 องค์ประกอบที่ช่วยในการตัดสินใจอย่างเหมาะสมในการใช้ฐานดังกล่าว ซึ่งจะต้องทำก่อนการประมวลผลข้อมูลส่วนบุคคล อันได้แก่

1. ระบุผลประโยชน์อันชอบธรรม (Identify a legitimate interest)

การประมวลผลข้อมูลส่วนบุคคลภายใต้ผลประโยชน์อันชอบธรรมอาจเป็นผลประโยชน์ของธนาคารเองหรือผลประโยชน์ของบุคคลที่สาม รวมถึงผลประโยชน์เชิงพาณิชย์ และผลประโยชน์แก่สาธารณะ

2. การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นต่อธนาคารในการบรรลุวัตถุประสงค์ (Show that the processing is necessary to achieve it)

การประมวลผลข้อมูลส่วนบุคคลจะต้องมีความจำเป็น หากธนาคารสามารถบรรลุวัตถุประสงค์เดียวกันได้อย่างสมเหตุสมผลด้วยวิธีการที่จะมีผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่น้อยกว่า ธนาคารควรประมวลผลโดยใช้ฐานอื่น

3. การรักษาสมดุลระหว่างผลประโยชน์อันชอบธรรมของธนาคารหรือผลประโยชน์ของบุคคลที่สาม กับประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Balance it against the individual's interests, rights and freedoms)

ธนาคารจะต้องชั่งน้ำหนักระหว่างผลประโยชน์อันชอบธรรมของธนาคารกับสิทธิเสรีภาพ/ประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หากการประมวลผลนั้นไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลแก่เจ้าของข้อมูลส่วนบุคคลหรืออาจก่อให้เกิดความไม่เป็นธรรม ธนาคารจะต้องให้ ประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลแทนที่ผลประโยชน์อันชอบธรรมของธนาคาร นั่นคือการให้สิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตามประโยชน์อันชอบธรรมของธนาคารไม่จำเป็นต้องสอดคล้องกับประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเสมอไป หากมีข้อโต้แย้งเกี่ยวกับสิทธิเสรีภาพ/ประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเกิดขึ้น ธนาคารยังสามารถประมวลผลได้เพื่อประโยชน์อันชอบธรรมดังกล่าวของธนาคารตราบเท่าที่ธนาคารจะแสดงให้เห็นอย่างสมเหตุสมผลและชัดเจนในเรื่องของผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง คำถามที่ใช้ประกอบการพิจารณาการทำ Balancing Test

- ธนาคารมีความสัมพันธ์อย่างไรกับเจ้าของข้อมูลส่วนบุคคล
- มีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลที่เป็นข้อมูลอ่อนไหวหรือข้อมูลส่วนบุคคลหรือไม่
- ลูกค้ามีความคาดหวังเกี่ยวกับกิจกรรมการประมวลผลของธนาคารในลักษณะนี้หรือไม่
- ธนาคารมีความเต็มใจและสามารถที่จะอธิบายเกี่ยวกับการประมวลผลให้ลูกค้าทราบหรือไม่
- ธนาคารคาดว่าลูกค้ามีแนวโน้มจะคัดค้านกิจกรรมการประมวลผลหรือพบว่าเป็นการละเมิด/รุกล้ำความเป็นส่วนตัวหรือไม่
- ผลกระทบที่เป็นไปได้ต่อบุคคลเป็นอย่างไรและจะมีผลกระทบมากน้อยเพียงใด
- ธนาคารกำลังประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์หรือไม่
- ธนาคารสามารถใช้มาตรการในการป้องกันเพื่อลดผลกระทบที่อาจเกิดขึ้นได้หรือไม่
- ธนาคารสามารถให้ลูกค้าทำการคัดค้านการประมวลผลได้หรือไม่

นอกจากนั้นธนาคารจะต้องทำการเก็บบันทึกประเมินการใช้ฐานผลประโยชน์อันชอบธรรม (LIA) เพื่อให้มั่นใจว่าการประมวลผลมีความจำเป็นและมีความสมเหตุสมผลในการใช้ฐานดังกล่าวเพื่อใช้แสดงแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลหากมีความจำเป็น และธนาคารจะต้องทำการระบุกิจกรรมการประมวลผล (Data Processing Activities) ที่ใช้ฐาน

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ผลประโยชน์อันชอบธรรมไว้ในนโยบายความเป็นส่วนตัวของธนาคาร (Privacy Notice) เพื่อเป็นการแจ้งให้ทราบแก่บุคคล

ในทางปฏิบัติธนาคารสามารถใช้ฐานการประมวลผลอันชอบธรรมได้ในกรณีต่อไปนี้

- ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาดได้ หากธนาคารสามารถแสดงให้เห็นถึงความเหมาะสมในการใช้ข้อมูล และมีผลกระทบเพียงเล็กน้อยต่อความเป็นส่วนตัวของบุคคล และบุคคลสามารถคาดหมายต่อกิจกรรมเหล่านั้นของธนาคารได้ หรือบุคคลไม่มีแนวโน้มที่จะคัดค้านกิจกรรมการประมวลผลเหล่านั้นได้
- ธนาคารสามารถประมวลผลข้อมูลของผู้เยาว์ภายใต้ฐานประโยชน์อันชอบธรรมได้ แต่จะต้องกระทำอย่างระมัดระวังเป็นพิเศษเพื่อให้แน่ใจว่าสิทธิและผลประโยชน์ของผู้เยาว์นั้นได้รับการคุ้มครองอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการทำโปรไฟล์ลิ่งข้อมูลของผู้เยาว์ ที่เกี่ยวกับการวิเคราะห์ข้อมูลเพื่อวัตถุประสงค์ทางการตลาด สำหรับกรณีนี้ธนาคารอาจต้องพิจารณาการจัดทำ DPIA เนื่องจากการทำโปรไฟล์ลิ่งข้อมูลของผู้เยาว์เข้าข่ายการพิจารณาการจัดทำ DPIA ตามเกณฑ์ของ GDPR เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประมวลผลข้อมูลและแนวทางในการจัดการกับความเสี่ยงดังกล่าว โปรดดูรายละเอียดการจัดทำ DPIA เพิ่มเติมในหัวข้อ “13. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)”

ตัวอย่างการใช้ฐานผลประโยชน์อันชอบธรรม

ตัวอย่าง 1 ธนาคารทำการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาด อันได้แก่ การวิเคราะห์ข้อมูล (Data Analytic) หรือใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ในประเภทเดียวกันกับที่ลูกค้ามีอยู่กับธนาคารและผลิตภัณฑ์อื่นของธนาคาร เพื่อให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น ธนาคารสามารถทำได้ภายใต้ฐานผลประโยชน์อันชอบธรรมของธนาคารหากพิสูจน์ได้ว่าผลประโยชน์อันชอบธรรมของธนาคารหรือของบุคคลที่สามมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล และธนาคารจะต้องแจ้งรายละเอียดหรือวิธีการใด ๆ ที่ให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์ในการปฏิเสธการรับข่าวสาร (Opt-out) หรือใช้สิทธิคัดค้านการประมวลผลได้ โดยการใช้สิทธินั้นสามารถทำได้ผ่านช่องทางการติดต่อที่ง่ายและสะดวกในการจัดการและการเข้าถึง

ตัวอย่าง 2 ธนาคารทำการประมวลผลข้อมูลส่วนบุคคล เพื่อการป้องกันระบบเศรษฐกิจการเงินในการจัดการอาชญากรรม การระงับเหตุ การสืบสวน การเรียกคืนความเสียหาย ลดความเสี่ยงทุจริตที่อาจเกิดการกระทำที่ผิดกฎหมายต่าง ๆ เพื่อป้องกันนักลงทุนและคุ้มครองสิทธิ ประโยชน์อันชอบธรรมของลูกค้าจากกลุ่มมิจฉาชีพที่แอบแฝงเข้าก่อความเสียหายต่อประชาชนทั้งทางตรงและทางอ้อมอันส่งผลถึงเศรษฐกิจโดยรวมของประเทศ เพื่อเสถียรภาพและความเชื่อมั่นต่อการจัดการอาชญากรรมทางเศรษฐกิจ ซึ่งรวมถึงการแบ่งปันข้อมูลส่วนบุคคลเพื่อยกระดับมาตรฐานการทำงานของกลุ่มสถาบันการเงินธุรกิจธนาคาร ในการป้องกันระงับเหตุ ลดความเสี่ยงทุจริตและกฎหมายอาญาข้างต้น เช่น การตรวจสอบป้องกันการทุจริต (Fraud Prevention and Investigation) ธนาคารอาจมีการเปิดเผยข้อมูลของบุคคลที่มีความเสี่ยงหรือบุคคลเฝ้าระวังที่เกี่ยวข้องกับการทุจริตหรือมีประวัติการทุจริตให้กับกลุ่มสถาบันการเงินธุรกิจธนาคาร รวมถึงการจัดเก็บและรวบรวมข้อมูล Fraud Risk ซึ่งอยู่ภายใต้ วัตถุประสงค์และนโยบายของกลุ่มธุรกิจธนาคาร หรือภายใต้วัตถุประสงค์และนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการของธนาคาร หากเป็นการเปิดเผยข้อมูลภายในเครือกิจการ เพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ข้างต้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตัวอย่าง 3 ธนาคารทำการบันทึกภาพบรรยากาศและบันทึกวีดีโอ ของผู้ที่มาเข้าร่วมการอบรมหรืองานสัมมนาต่างๆ ซึ่งการบันทึกดังกล่าวอาจมีการเปิดเผยหรือเผยแพร่ให้แก่บุคคลภายนอกเพื่อวัตถุประสงค์ในการประชาสัมพันธ์ อย่างไรก็ตามสำหรับกรณีนี้ธนาคารจะต้องทำการติดประกาศในบริเวณงานเพื่อเป็นการแจ้งให้ทราบแก่บุคคลที่มาร่วมงาน ว่าจะมีการบันทึกภาพในงานและอาจมีการเผยแพร่เพื่อการประชาสัมพันธ์

ตัวอย่าง 4 ธนาคารทำการประมวลผลข้อมูลส่วนบุคคลเพื่อการรักษาความสัมพันธ์กับลูกค้า เช่น การจัดการข้อร้องเรียน การเสนอสิทธิประโยชน์พิเศษโดยไม่มีวัตถุประสงค์ทางการตลาดให้แก่ลูกค้า เป็นต้น

ตัวอย่าง 5 ธนาคารทำการบันทึกภาพผู้ที่มาติดต่อทำธุรกรรมกับสำนักงานหรือสาขาของธนาคารลงบน CCTV รวมถึง การแลกบัตรก่อนเข้าอาคาร เพื่อการรักษาความปลอดภัยภายในบริเวณอาคารของธนาคาร อย่างไรก็ตามสำหรับกรณีนี้ธนาคารจะต้องทำการติดประกาศ ในบริเวณที่สามารถเห็นได้ง่ายของอาคาร เพื่อเป็นการแจ้งให้ทราบ

ตัวอย่าง 6 ธนาคารมีการติดกล้องที่ตู้ ATM และมีการบันทึกภาพ เพื่อวัตถุประสงค์ในการรักษาความปลอดภัย อย่างไรก็ตามธนาคารควรติดประกาศหรือแจ้งผ่านหน้าจอแสดงผล เพื่อเป็นการแจ้งให้ทราบแก่บุคคลที่มาใช้บริการผ่านตู้ ATM

ตัวอย่าง 7 ธนาคารทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการบริหารความเสี่ยง/การกำกับตรวจสอบ/การบริหารจัดการภายในองค์กร เช่น ข้อมูลบุคคลล้มละลาย, ข้อมูลบุคคลที่มีความเสี่ยงในการทุจริต Fraud Risk, ข้อมูลรายชื่อลูกค้าเฝ้าระวัง Suspect risk ของธนาคารให้กับบริษัทในเครือกิจการซึ่งอาจอยู่ในราชอาณาจักรและนอกราชอาณาจักร (Intra-Group Transfer) เพื่อวัตถุประสงค์ดังกล่าว โดยธนาคารอาจจัดให้มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules) ที่ได้รับการรับรองจากสำนักงาน หรือข้อตกลง

ตัวอย่าง 9 ธนาคารทำการแจ้งเตือน (Payment Reminder) เพื่อการชำระหนี้/ต่ออายุผลิตภัณฑ์ของบริษัทที่ธนาคารเป็นนายหน้า เช่น ผลิตภัณฑ์กองทุน กรมธรรม์ เป็นต้น

ตัวอย่าง 10 ธนาคารทำการแจ้งเตือน (Payment Reminder) เพื่อชำระค่าบริการต่าง ๆ (Bill Payment) ให้แก่บริษัทที่ลูกค้าใช้บริการ ซึ่งอาจเป็นรายการที่เกิดขึ้นบ่อยครั้ง เช่น ค่าน้ำ ค่าไฟ

ตัวอย่าง 11 ธนาคารทำการบันทึกเสียงผ่านทาง Contact Center เพื่อใช้ในการรับเรื่องร้องเรียน และเพื่อปรับปรุงการให้บริการที่ดีขึ้น อย่างไรก็ตามธนาคารจะต้องทำการแจ้งแก่บุคคลที่ทำการติดต่อก่อนดำเนินการบันทึกเสียง ว่าธนาคารจะทำการบันทึกเสียง

ตัวอย่าง 12 สำหรับ Mobile Banking Application กรณีธนาคารแสดงข้อมูลของบุคคลอื่นในรายการโปรดภายในแอปพลิเคชัน เป็นการแสดงข้อมูลของบุคคลอื่นเพื่ออำนวยความสะดวกให้แก่ลูกค้า

ตัวอย่าง 13 ธนาคารอาจบริการแจ้งเตือนลูกค้าผ่านช่องทางต่าง ๆ เช่น ส่งข้อความอีเมลหรือโทรติดต่อลูกค้า ในกรณีที่มีการทำธุรกรรมผ่านตู้ ATM, Online Banking การใช้จ่ายผ่านบัตรเครดิต และอื่น ๆ ที่มีจำนวนเงินหรือรูปแบบการทำธุรกรรม ที่เข้าข่ายรายการที่ผิดปกติ ลูกค้าจะได้รับข้อมูลเกี่ยวกับบัญชี หรือการสอบถามการทำรายการจากธนาคาร ซึ่งจะเป็นประโยชน์ต่อธนาคารและลูกค้าในการลดความเสี่ยงจากการทำธุรกรรมที่ไม่สุจริต

ตัวอย่าง 14 ธนาคารทำการส่งข้อมูลเกี่ยวกับงานอบรมหรือสัมมนาต่าง ๆ เพื่อเป็นการประชาสัมพันธ์โครงการให้แก่กลุ่มลูกค้าของธนาคารที่อาจสนใจเข้าร่วมโครงการ

ตัวอย่างที่ 15 ในกรณีที่จะขอให้ลูกค้าทำการตอบแบบสอบถามในการสำรวจความพึงพอใจในการให้บริการของธนาคารเพื่อให้ธนาคารนำไปใช้ในการปรับปรุงและพัฒนาผลิตภัณฑ์และการบริการให้ตรงต่อความต้องการและดียิ่งขึ้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5.2.6 ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

ฐานการปฏิบัติตามกฎหมาย ผู้ควบข้อมูลส่วนบุคคลสามารถใช้ฐานดังกล่าวได้ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลตามที่กฎหมายกำหนด และจะต้องสามารถระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใด สำหรับกรณีนี้ แม้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีสิทธิในการคัดค้านการประมวลผลข้อมูล อย่างไรก็ตามหากการประมวลผลดังกล่าวเป็นไปตามฐานการปฏิบัติตามกฎหมาย ธนาคารสามารถปฏิเสธคำร้องขอการคัดค้านการประมวลผลได้ โดยการระบุเหตุแห่งการปฏิเสธประกอบด้วย

ตัวอย่าง 1 ธนาคารมีความจำเป็นอย่างยิ่งในการประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในการระบุตัวตนและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า Know Your Customer (KYC), Customer Due Diligence (CDD) เพื่อปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

ตัวอย่าง 2 ธนาคารมีหน้าที่ในการจัดทำการยื่นภาษีให้กับกรมสรรพากร ซึ่งกรมสรรพากรอาจขอให้ธนาคารเปิดเผยข้อมูลค่าใช้จ่ายเงินเดือนพนักงาน เพื่อทำการตรวจสอบความถูกต้องของข้อมูลในการคำนวณภาษีที่ธนาคารยื่นต่อกรมสรรพากร กรณีนี้ธนาคารสามารถเปิดเผยข้อมูลให้กับกรมสรรพากรภายใต้ฐานการปฏิบัติตามกฎหมาย

ตัวอย่าง 3 ธนาคารเปิดเผยข้อมูลสินทรัพย์และหนี้สินของพนักงานหรือลูกค้าให้กับคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เพื่อให้สำนักงานใช้ในการตรวจสอบความถูกต้องของรายการสินทรัพย์หนี้สิน ภายใต้กฎหมายป้องกันและปราบปรามการทุจริต

ตัวอย่าง 4 ในกรณีที่ธนาคารมีความจำเป็นจะต้องเปิดเผยข้อมูลส่วนบุคคลของลูกหนี้แก่ศาล เพื่อดำเนินการฟ้องล้มละลายภายใต้พระราชบัญญัติล้มละลาย

ตัวอย่าง 5 เพื่อปฏิบัติตามข้อกำหนดของกฎหมาย Foreign Account Tax Compliance Act (FATCA) ตามที่ประเทศไทยได้ทำข้อตกลงกับประเทศสหรัฐฯ ธนาคารอาจมีความจำเป็นต้องเก็บรวบรวมข้อมูลสัญชาติของลูกค้า และมีหน้าที่ตามกฎหมายที่ต้องรายงานข้อมูลทางบัญชีของลูกค้าชาวอเมริกันต่อกรมสรรพากรของสหรัฐฯ ในกรณีที่ธนาคารมีการดำเนินงานในลักษณะที่เป็นการสร้างรายได้หรือผลกำไรให้กับชาวสหรัฐฯ

5.2.7 ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research)
กรณีที่ธนาคารมีความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือสาธารณประโยชน์อื่น ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น สำหรับการประมวลผลโดยฐานนี้ GDPR กำหนดให้จะต้องใช้ฐานอื่นประกอบการประมวลผลโดยฐานนี้เสมอ ไม่สามารถอ้างฐานนี้เพียงอย่างเดียวเพื่อใช้ในการประมวลผลได้นอกจากนั้นการประมวลผลบนฐานนี้มีความจำเป็นที่จะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด เนื่องจากการประมวลผลข้อมูลภายใต้ฐานนี้จำเป็นจะต้องมีมาตรการที่ความสอดคล้องกับมาตรฐานจริยธรรม และระเบียบในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติด้วย

5.3 ความยินยอม (Consent)

5.3.1 เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้
- เจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อใดก็ได้
- การใช้ฐานความยินยอมนั้น จะต้องให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถปฏิเสธไม่ให้ความยินยอมได้
- การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้น ธนาคารจึงควรออกแบบแบบฟอร์มการขอความยินยอมที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเห็นได้อย่างชัดเจนว่า ธนาคารขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง
- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) หรือข้อความในสัญญา
- การขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

5.3.2 การใช้ฐานความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นฐานในการประมวลผลที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะจัดการกับข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ของตนเองได้อย่างเต็มที่ ซึ่งธนาคารจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการประมวลผล ยกเว้นกรณีการประมวลผลข้อมูลส่วนบุคคลเป็นการประมวลผลภายใต้ฐานกฎหมายอื่น

5.3.3 ธนาคารควรเลือกใช้ฐานในการประมวลผลให้เหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล เนื่องจากฐานความยินยอมไม่สามารถใช้ได้กับทุกกรณี เว้นแต่กรณีที่ต้องขอความยินยอมตามข้อกำหนดของกฎหมายอื่น ฐานความยินยอมจะเหมาะสมเมื่อการประมวลผลข้อมูลไม่ได้มีความจำเป็นตามเงื่อนไขของสัญญา นอกจากนั้นการให้ความยินยอมจะต้องเป็นสิ่งที่ให้เจ้าของข้อมูลส่วนบุคคลทำการเลือกว่าจะให้หรือปฏิเสธได้ และการปฏิเสธจะต้องไม่มีผลกระทบต่อการได้รับบริการตามสัญญา การขอความยินยอมจะต้องกระทำโดยชอบด้วยกฎหมาย เป็นธรรม และโปร่งใสตามหลักการ Principle 1 : (“Lawfulness, Fairness, and Transparency”) โดยธนาคารจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ และจะต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการตัดสินใจให้ความยินยอม โดยการให้ความยินยอมจะต้องเป็นการสมัครใจ ดังนั้นการขอความยินยอมจะต้องระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด

5.3.4 ธนาคารต้องไม่นำฐานความยินยอมและฐานสัญญามาปะปนกัน ต้องแยกให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาก็ควรจะระบุอยู่ในสัญญา ซึ่งการขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) เนื่องจากการกระทำดังกล่าวอาจทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการหรือมีผลต่อการใช้ผลิตภัณฑ์หรือบริการของธนาคาร

5.3.5 นอกจากนั้นการใช้ฐานความยินยอมอาจเหมาะสมในสถานการณ์ที่จะประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เฉพาะเจาะจงมากกว่า และธนาคารไม่สามารถประมวลผลตามวัตถุประสงค์ที่เพิ่มเติมขึ้นมาใหม่เองได้ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ธนาคารจะต้องทำการขอความยินยอมใหม่หากต้องการประมวลผลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว เว้นแต่หากพิจารณาแล้วว่าการประมวลผลเพื่อวัตถุประสงค์อื่นนั้น สามารถทำได้ภายใต้ฐานกฎหมายฐานอื่น

5.3.6 การขอความยินยอม สามารถทำได้หลายวิธี เช่น

- การยินยอมจากการเลือกยินยอม (Opt-in Consent) ผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน เป็นลายลักษณ์อักษร ธนาคารควรออกแบบให้เจ้าของข้อมูลส่วนบุคคลต้องมีการกระทำให้ความยินยอม

อย่างชัดเจน (Clear Affirmative Action) เช่น การทำเป็นช่องเช็คถูก (Check Box) โดยให้เจ้าของข้อมูลส่วนบุคคลกด/เขียนเช็คเองได้ (Signatures or Ticks Indicating Consent)

- การขอความยินยอมในรูปแบบวาจา (Verbal Consent) สำหรับรูปแบบการขอความยินยอมนี้ใช้ในกรณีที่มีการบันทึกความยินยอมในรูปแบบเสียง (Voice Record) ด้วยระบบดิจิทัล เช่น บันทึกผ่านการติดต่อกับเจ้าของข้อมูลส่วนบุคคลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลส่วนบุคคลกดปุ่มยืนยันการให้ความยินยอม เป็นต้น ซึ่งธนาคารจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลส่วนบุคคลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลส่วนบุคคลของธนาคารจริง นอกจากนั้นธนาคารควรให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลอย่างเพียงพอต่อการตัดสินใจ มีทางเลือก และเนื้อหาชัดเจนไม่ก่อให้เกิดความเข้าใจผิด และให้เจ้าของข้อมูลส่วนบุคคลสามารถให้ความยินยอมหรือไม่ให้ความยินยอมก็ได้โดยสมัครใจ ไม่เป็นการบังคับ
- การถอนความยินยอม (Withdraw of Consent)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอเพิกถอนความยินยอม (“Right to Withdraw of Consent”) ที่จะให้ไว้กับธนาคารในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และธนาคารจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้หากธนาคารไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวมใช้หรือเปิดเผยต่อไปให้ธนาคารดำเนินการลบข้อมูลออก

การใช้สิทธิถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

5.3.7 กรณีการเก็บรวบรวมข้อมูลส่วนบุคคล ที่ธนาคารสามารถทำได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอม ในกรณีดังนี้

- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุหรือเพื่อประโยชน์สาธารณะ
- เพื่อการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของธนาคาร หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ธนาคาร
- เป็นการจำเป็นเพื่อประโยชน์อันชอบด้วยกฎหมายของธนาคารหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ธนาคาร เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่างการประมวลผลข้อมูลที่ควรใช้ฐานความยินยอม

ตัวอย่าง 1 ธนาคารจะต้องทำการขอความยินยอม เพื่อใช้ในการเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินอื่น ๆ ของลูกค้าที่ได้ให้ไว้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น ไปยังกลุ่มธุรกิจทางการเงินของธนาคาร และพันธมิตรทางธุรกิจของธนาคาร เพื่อการส่งเสริมการขายผลิตภัณฑ์และบริการ และเพื่อประชาสัมพันธ์เกี่ยวกับบริการต่าง ๆ (Marketing Purpose) ของบุคคลดังกล่าว สำหรับกรณีนี้ธนาคารต้องขอความยินยอมจากลูกค้าภายใต้ข้อกำหนดของประกาศธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market conduct)

ตัวอย่าง 2 ธนาคารต้องการเก็บรวบรวมข้อมูลทางชีวมิติ (Biometric) เช่น ข้อมูลแบบจำลองใบหน้า (Face recognition), ข้อมูลแบบจำลองลายนิ้วมือ เป็นต้น ซึ่งเป็นข้อมูลอ่อนไหวเพื่อใช้ในการยืนยันตัวตนของลูกค้าในขั้นตอนการสมัครครั้งแรก หรือการยืนยันตัวตนก่อนการใช้บริการผลิตภัณฑ์ดิจิตัล ธนาคารจะต้องทำการขอความยินยอมในการประมวลผลข้อมูลอ่อนไหวก่อนหรือขณะที่ลูกค้าสมัครใช้บริการครั้งแรก เนื่องจากการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวจะต้องขอความยินยอมโดยชัดแจ้ง ในกรณีที่เป็นผลิตภัณฑ์ดิจิทัลที่ไม่มีช่องทางอื่นในการยืนยันตัวตนสำหรับผลิตภัณฑ์ ธนาคารสามารถระบุเงื่อนไขไว้ในการขอความยินยอมได้ว่าหากไม่ให้ข้อมูลดังกล่าวธนาคารก็จะไม่สามารถให้บริการได้เนื่องจากมีความจำเป็นในการให้บริการอย่างไร

ตัวอย่างกรณีการขอความยินยอมที่ไม่ควรนำมารวมอยู่ในเงื่อนไขของการให้บริการ

ตัวอย่าง 1 ลูกค้าทำการสมัครบัตรเครดิตกับธนาคาร ธนาคารไม่สามารถกำหนดให้ลูกค้าจะต้องให้ความยินยอมในการรับข้อมูลข่าวสารทางการตลาด ที่เป็นการนำเสนอผลิตภัณฑ์ในประเภทเดียวกันกับที่ลูกค้ามีอยู่กับธนาคารและผลิตภัณฑ์อื่นของธนาคาร ไว้ในเงื่อนไขของการสมัครบัตรเครดิตได้ เนื่องจากการขอความยินยอมดังกล่าวไม่เกี่ยวข้องและเกินความจำเป็นในการให้บริการบัตรเครดิต อย่างไรก็ตามสำหรับกรณีนี้ธนาคารอาจไม่จำเป็นต้องขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในการนำเสนอผลิตภัณฑ์ในประเภทเดียวกันกับที่ลูกค้ามีอยู่กับธนาคารและผลิตภัณฑ์อื่นของธนาคาร ธนาคารสามารถทำได้ภายใต้ฐานผลประโยชน์อันชอบธรรมของธนาคารหากพิสูจน์ได้ว่าผลประโยชน์อันชอบธรรมของธนาคารหรือของบุคคลที่สามมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล และธนาคารจะต้องแจ้งรายละเอียดหรือวิธีการใด ๆ ที่ให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์ในการปฏิเสธการรับข่าวสาร (Opt-out) หรือใช้สิทธิคัดค้านการประมวลผลได้ โดยการใช้สิทธินั้นสามารถทำได้ผ่านช่องทางการติดต่อที่ง่ายและสะดวกในการจัดการและการเข้าถึงรวมทั้งมีกระบวนการภายในที่จะรวบรวมข้อมูลลูกค้าที่จะไม่ประสงค์รับการติดต่อจากธนาคารในการขายผลิตภัณฑ์ได้

ตัวอย่าง 2 ธนาคารไม่สามารถกำหนดให้การขายผลิตภัณฑ์ด้านหลักทรัพย์หรือประกันภัยควบคู่กับผลิตภัณฑ์ของธนาคารได้ (Bundle Product) หรือกำหนดเป็นเงื่อนไขในการขายหรือให้บริการผลิตภัณฑ์หลัก เช่น ให้ลูกค้าทำประกันภัยกับบริษัทใดบริษัทหนึ่งเพื่อเป็นเงื่อนไขในการพิจารณาการให้สินเชื่อ ในกรณีนี้หากธนาคารต้องการเสนอขายผลิตภัณฑ์ด้านหลักทรัพย์และประกันภัย สามารถทำได้ภายใต้ความเหมาะสม แต่ธนาคารจะต้องแจ้งรายละเอียดหรือวิธีการใด ๆ ที่ให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์ในการปฏิเสธการรับข่าวสาร หรือใช้สิทธิคัดค้านการประมวลผลได้ โดยการใช้สิทธินั้นสามารถทำได้ผ่านช่องทางการติดต่อที่ง่ายและสะดวกในการจัดการและการเข้าถึงรวมทั้งมีกระบวนการภายในที่จะรวบรวมข้อมูลลูกค้าที่จะไม่ประสงค์รับการติดต่อจากธนาคารในการขายผลิตภัณฑ์ได้

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

<u>ตัวอย่าง แบบฟอร์มการขอความยินยอม (Consent form)</u>

<u>หนังสือให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)</u>

เรียนลูกค้าคนสำคัญ:

ธนาคารมีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาท่านไปสู่ความปลอดภัยทางการเงิน และยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด ให้สอดคล้องกับกฎหมายและกฎระเบียบข้อบังคับ ธนาคารจึงได้จัดทำหนังสือขออนุญาตจากท่านในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของท่าน ที่ท่านได้ให้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น เพื่อวัตถุประสงค์ดังต่อไปนี้:

- [ ]

ท่านสามารถดูรายละเอียดเพิ่มเติมที่เผยแพร่ภายใต้ นโยบายความเป็นส่วนตัว (Privacy Policy) บนเว็บไซต์ของธนาคาร <webpage URL> ธนาคารจะทำการเก็บข้อมูลส่วนบุคคลและการให้ความยินยอมของลูกค้าไว้ตามนโยบายของธนาคาร หากท่านประสงค์จะเพิกถอนความยินยอมนี้ หรือทำการยื่นข้อร้องเรียนใด ๆที่เกี่ยวกับการละเมิดสิทธิของท่าน สามารถดำเนินการผ่านทาง ABC Contact Center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของธนาคาร นอกจากนี้ท่านยังสามารถรายงานหรือยื่นข้อเรื่องร้องเรียนใด ๆที่เกี่ยวข้องกับการละเมิดสิทธิของท่าน ได้ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ DPO@abcbank.com

วันที่.....

ชื่อ-นามสกุล……

เบอร์ติดต่อ..... Email.....

☐ ยินยอม ☐ ไม่ยินยอม

ลงชื่อ.....เจ้าของข้อมูลส่วนบุคคล

(.....)

<u>หนังสือให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)</u>

ธนาคารมีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาท่านไปสู่ความปลอดภัยทางการเงิน และยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด อีกทั้งยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด ให้สอดคล้องกับกฎหมายและกฎระเบียบข้อบังคับ ธนาคารจึงได้จัดทำหนังสือขออนุญาตจากท่านในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของท่าน ที่ท่านได้ให้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น เพื่อวัตถุประสงค์ดังต่อไปนี้:

- เพื่อใช้ในการยืนยันตัวตนของลูกค้า โดยการสแกนใบหน้า/ สแกนลายนิ้วมือ (Biometric) เพื่อเข้าใช้บริการ Application ของธนาคารแทนการเข้ารหัส

ท่านสามารถดูรายละเอียดเพิ่มเติมที่เผยแพร่ภายใต้ นโยบายความเป็นส่วนตัว (Privacy Nolicy) บนเว็บไซต์ของธนาคาร <webpage URL> ธนาคารจะทำการเก็บข้อมูลส่วนบุคคลและการให้ความยินยอมของลูกค้าไว้ตามนโยบายของธนาคาร หากท่านประสงค์จะเพิกถอนความยินยอมนี้ หรือทำการยื่นข้อร้องเรียนใดๆที่เกี่ยวกับการละเมิดสิทธิของท่าน สามารถดำเนินการผ่านทาง ABC Contact center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของธนาคาร นอกจากนี้ท่านยังสามารถรายงานหรือยื่นข้อเรื่องร้องเรียนใดๆที่เกี่ยวข้องกับการละเมิดสิทธิของท่าน ได้ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ DPO@abcbank.com

วันที่.....

ชื่อ-นามสกุล……..……

เลขประจำตัวประชาชน.....หนังสือเดินทางเลขที่ (กรณีคนต่างด้าว).....

☐ ยินยอม ☐ ไม่ยินยอม

ลงชื่อ ..... เจ้าของข้อมูลส่วนบุคคล

(.....)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

<u>หนังสือให้ความยินยอมในการเก็บรวบรวม/ใช้/เปิดเผยข้อมูลส่วนบุคคล (PDPA)</u>

ธนาคารมีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาท่านไปสู่ความปลอดภัยทางการเงิน และยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด ให้สอดคล้องกับกฎหมายและกฎระเบียบข้อบังคับ ธนาคารจึงได้จัดทำหนังสือขออนุญาตจากท่านในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของท่าน ที่ท่านได้ให้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น เพื่อวัตถุประสงค์ดังต่อไปนี้:

1. [ ]
2. [ ]

ท่านสามารถดูรายละเอียดเพิ่มเติมที่เผยแพร่ภายใต้ นโยบายความเป็นส่วนตัว (Privacy Policy) บนเว็บไซต์ของธนาคาร <webpage URL> ธนาคารจะทำการเก็บข้อมูลส่วนบุคคลและการให้ความยินยอมของลูกค้าไว้ตามนโยบายของธนาคาร หากท่านประสงค์จะเพิกถอนความยินยอมนี้ หรือทำการยื่นข้อร้องเรียนใดๆที่เกี่ยวกับการละเมิดสิทธิของท่าน สามารถดำเนินการผ่านทาง ABC Contact Center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของธนาคาร นอกจากนี้ท่านยังสามารถรายงานหรือยื่นข้อเรื่องร้องเรียนใดๆที่เกี่ยวข้องกับการละเมิดสิทธิของท่าน ได้ที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ DPO@abcbank.com

วันที่.....

ชื่อ-นามสกุล……

เลขประจำตัวประชาชน.....หนังสือเดินทางเลขที่ (กรณีคนต่างด้าว).....

☐ ยินยอม ☐ ไม่ยินยอม

ลงชื่อ ..... เจ้าของข้อมูลส่วนบุคคล

(.....)

<u>หนังสือยินยอมให้เปิดเผยข้อมูลเพื่อวัตถุประสงค์ทางการตลาด (Market Conduct)</u>

ธนาคารมีความมั่นใจเป็นอย่างยิ่งว่าจะนำพาท่านไปสู่ความปลอดภัยทางการเงิน และยังคงนำเสนอผลิตภัณฑ์และบริการที่เหมาะสมกับท่านมากที่สุด ให้สอดคล้องกับกฎหมายและกฎระเบียบข้อบังคับ ธนาคารจึงได้จัดทำหนังสือขออนุญาตจากท่านในการเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลทางการเงินอื่น ๆ ของท่าน ที่ท่านได้ให้แก่ธนาคารหรือที่ธนาคารอาจเข้าถึงได้จากแหล่งอื่น ไปยังบุคคลดังต่อไปนี้:

1. [ ]
2. [ ]

ข้อมูลส่วนบุคคลของท่านที่ถูกเปิดเผยไปยังบุคคลดังกล่าวข้างต้น จะถูกนำไปใช้เพื่อการส่งเสริมการขายผลิตภัณฑ์และบริการอื่น และเพื่อประชาสัมพันธ์เกี่ยวกับบริการต่างๆ หากท่านประสงค์จะเพิกถอนความยินยอมนี้ หรือทำการยื่นข้อร้องเรียนใดๆที่เกี่ยวกับการละเมิดสิทธิของท่าน สามารถดำเนินการผ่านทาง ABC Contact Center หมายเลข 1234 หรือช่องทางที่ระบุไว้ในเว็บไซต์ของธนาคาร

*ท่านมีสิทธิเลือกให้ความยินยอมหรือไม่ก็ได้ โดยไม่ส่งผลต่อการพิจารณาการใช้ผลิตภัณฑ์หรือบริการของธนาคาร

วันที่.....

ชื่อ-นามสกุล.....

เลขประจำตัวประชาชน.....หนังสือเดินทางเลขที่ (กรณีคนต่างด้าว).....

☐ ยินยอม ☐ ไม่ยินยอม

ลงชื่อ ..... เจ้าของข้อมูลส่วนบุคคล

(.....)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5.3.8 การขอความยินยอมจากผู้เยาว์

ในการขอความยินยอมจากผู้เยาว์ (ผู้เยาว์หมายถึง ผู้มีอายุไม่ครบ 20 ปีบริบูรณ์ หรือ ไม่ได้จดทะเบียนสมรสกันก่อนอายุ 20 ปีโดยอายุไม่ต่ำกว่า 17 ปี) ธนาคารต้องกระทำโดยระมัดระวังเป็นพิเศษ เนื่องจากความสามารถในการเข้าใจวัตถุประสงค์ของผู้เยาว์นั้นไม่เท่ากับผู้ที่บรรลุนิติภาวะแล้ว ดังนั้นการขอความยินยอมจากผู้เยาว์ต้องทำอย่างถูกต้อง เป็นธรรมและโปร่งใส Principle 1 : ("Lawfulness, Fairness, and Transparency") โดยใช้ภาษาที่ง่าย มีความเหมาะสมกับระดับความเข้าใจของผู้เยาว์ มีความชัดเจน ไม่ก่อให้เกิดความเข้าใจผิดได้ง่าย

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลได้ให้หลักการในเรื่องของการให้ความยินยอมของผู้เยาว์ว่า หากเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา 27 แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากผู้เยาว์นั้น จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำแทนผู้เยาว์ด้วย เว้นแต่ เป็นไปตาม มาตรา 22 23 และ 24* แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์จึงจะสามารถให้ความยินยอมตามลำพังได้

ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(* มาตรา 22 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อหลุดพ้นจากหน้าที่อันใดอันหนึ่ง

มาตรา 23 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการต้องทำเองเฉพาะตัว

มาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์อาจทำการใดๆ ได้ทั้งสิ้น ซึ่งเป็นการสมแก่ฐานานุรูปแห่งตน และเป็นการอันจำเป็นในการดำรงชีพอันสมควร)

สำหรับการถอนความยินยอมของผู้เยาว์ที่ไม่ใช่เพื่อการใด ๆ ตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 22 23 และ 24 จะต้องได้รับความยินยอมจากผู้มีอำนาจปกครองที่มีอำนาจกระทำแทนด้วย ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ใช้สิทธิในการถอนความยินยอมกระทำการแทนผู้เยาว์

หากธนาคารมีความจำเป็นที่ต้องประมวลผลข้อมูลของผู้เยาว์ ธนาคารควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ก่อนการประมวลผล โปรดดูรายละเอียดในหัวข้อ “13 แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)” เพื่อประเมินผลกระทบที่อาจเกิดขึ้น และหาวิธีการลดความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ต่อไป นอกจากนั้นธนาคารต้องคำนึงถึงการคุ้มครองสิทธิของผู้เยาว์ด้วย

ตัวอย่างกรณีมาตรา 22 มาตรา 23 และมาตรา 24 ในกรณีที่ลูกค้า(ผู้เยาว์) มีความประสงค์ที่จะเปิดบัญชีกับธนาคารและการทำบัตร ATM ในกรณีดังกล่าวข้างต้นลูกค้า (ผู้เยาว์) สามารถให้ความยินยอมโดยลำพังได้

5.3.9 การขอความยินยอมในการเก็บคุกกี้ (Cookie Consent)

“คุกกี้ (Cookie)” หมายถึง ข้อความขนาดเล็กที่เว็บไซต์ทำการเก็บไว้ ซึ่งคุกกี้จะถูกจัดเก็บลงในอุปกรณ์คอมพิวเตอร์ หรือเครื่องมือสื่อสารที่เข้าใช้งานของผู้ใช้งานเว็บไซต์หรือแอปพลิเคชัน ซึ่งคุกกี้จะถูกนำมาใช้เพื่อทำให้ผู้ใช้งานเว็บไซต์หรือแอปพลิเคชันสามารถใช้งานได้อย่างต่อเนื่อง อย่างไรก็ตาม คุกกี้บางประเภทอาจส่งผลกระทบกับความเป็นส่วนตัวของผู้ใช้งาน เช่น ใช้ในการวิเคราะห์ความสนใจลูกค้า พฤติกรรมการเยี่ยมชม เพื่อนำเสนอสื่อให้เหมาะสมกับความสนใจของลูกค้า รวมถึงอาจมีการติดตามการใช้งานเว็บไซต์หรือแอปพลิเคชันที่ผู้ใช้งานเยี่ยมชมได้

ธนาคารสามารถใช้ข้อมูลคุกกี้ประเภทที่มีความจำเป็นต่อการใช้งานเว็บไซต์หรือแอปพลิเคชัน (Necessary Cookies) ได้โดยไม่ต้องขอความยินยอม สำหรับคุกกี้ประเภทอื่น ๆ เช่น คุกกี้ที่ใช้ในการวิเคราะห์ข้อมูล (Analytic Cookies) คุกกี้ที่ใช้ในการโฆษณา (Targeting Cookies) เป็นต้น ธนาคารควรทำการขอความยินยอมในการใช้งานคุกกี้ประเภทที่ไม่ได้จำเป็นต่อการใช้งานเว็บไซต์ดังกล่าวก่อนการใช้คุกกี้นั้น ๆ หรือธนาคารอาจจัดให้ลูกค้าสามารถจัดการฟังก์ชันคุกกี้เองได้ กล่าวคือ ลูกค้าจะสามารถเลือกเปิดหรือปิดค่าคุกกี้แต่ละประเภทในหน้าเว็บไซต์ได้ ในการขอความยินยอมคุกกี้ ผู้ใช้งานจะต้องสามารถยอมรับหรือปฏิเสธคุกกี้ได้และการปฏิเสธไม่ให้ความยินยอมของผู้ใช้งานจะต้องไม่ส่งผลกระทบต่อการใช้งานเว็บไซต์หรือแอปพลิเคชัน

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5.4 ข้อมูลอ่อนไหว (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว "Sensitive Personal Data" คือ ข้อมูลส่วนบุคคลที่สามารถพิจารณาได้ว่าเป็นเรื่องส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และมีความละเอียดอ่อนและมีความสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการอย่างระมัดระวังเป็นพิเศษในการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ประวัติอาชญากรรม ความเห็นทางการเมือง ความเชื่อ ลัทธิ ศาสนา ปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลความพิการ ข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นใดซึ่งกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

ธนาคารห้ามเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Explicit Consent) เว้นแต่ในกรณีที่ได้รับการยกเว้นตามกฎหมายไม่ได้ต้องขอความยินยอม ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว ได้แก่

- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
- เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคมหรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอก
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านการสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นที่สำคัญ โดยต้องกระทำเพื่อบรรลุวัตถุประสงค์เท่าที่จำเป็น และจัดให้มีมาตรการในการคุ้มครองข้อมูลที่เหมาะสม

ในกรณีการเก็บ รวบรวม ใช้และเปิดเผยข้อมูลของผู้เปราะบางของธนาคารตามเกณฑ์ของธนาคารแห่งประเทศไทยและสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารสามารถเก็บ รวบรวม ใช้และเปิดเผยข้อมูลของผู้เปราะบางโดยไม่ต้องขอความยินยอมจากผู้เปราะบางโดยอาศัยมาตรา 26 (4)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตัวอย่าง 1 ในกรณีที่ลูกค้าทำการซื้อผลิตภัณฑ์ประกันภัยกับธนาคาร ธนาคารอาจมีความจำเป็นที่ต้องทำการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพของลูกค้าในปัจจุบัน, ประวัติสุขภาพ ในกรณีเหล่านี้ธนาคารจำเป็นต้องได้รับความยินยอมอย่างชัดแจ้งจากลูกค้าก่อนหรือขณะเก็บรวบรวมข้อมูล

ตัวอย่าง 2 ในกรณีของกลุ่มธนาคาร ที่ต้องทำการเก็บข้อมูลจากบัตรประจำตัวประชาชนซึ่งมีข้อมูลอ่อนไหวคือศาสนา และ/หรือกรุ๊ปเลือด เพื่อวัตถุประสงค์ในการยื่นคำขอเปิดบัญชีธนาคาร และเพื่อการบริหารจัดการบัญชี ซึ่งเกิดขึ้นบ่อยครั้งในรูปแบบของ

- การขอถ่ายสำเนาบัตรประจำตัวประชาชนจากลูกค้า และเก็บสำเนาของข้อมูลลูกค้าไว้
- การอ่านข้อมูลทางอิเล็กทรอนิกส์บนชิพการ์ดของบัตรประจำตัวประชาชน และเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์เข้าฐานข้อมูลของธนาคาร

หากธนาคารจะทำการเก็บรวบรวมข้อมูลศาสนา จะต้องได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือหากธนาคารไม่ประสงค์จะขอความยินยอมจากลูกค้า ก็จะต้องมีกระบวนการในการจัดเก็บข้อมูลบัตรประจำตัวประชาชน โดยไม่มีการเก็บข้อมูลศาสนา และ/หรือกรุ๊ปเลือด เช่นการขีดทึบข้อมูลดังกล่าวในสำเนาบัตรประจำตัวประชาชน

ตัวอย่าง 3 กรณีที่ธนาคารเก็บรวบรวมข้อมูลอ่อนไหว อันได้แก่ลายนิ้วมือของพนักงานเพื่อใช้ในการเช็คเวลาเข้างานหรือเลิกงาน หรือ ใช้การสแกนลายนิ้วมือเพื่อเข้าตึกสำนักงานของธนาคาร ธนาคารจะต้องทำการขอความยินยอมอย่างชัดแจ้งในการเก็บข้อมูลลายนิ้วมือ เมื่อพนักงานเข้าทำงานกับธนาคาร สำหรับข้อมูลลายนิ้วมือที่มีการเก็บอยู่ก่อนแล้วให้ธนาคารทำการขอความยินยอมใหม่

ตัวอย่าง 4 กรณีลูกจ้างลาป่วยติดต่อกันเกิน 3 วัน ลูกจ้างจะต้องแสดงใบรับรองแพทย์ตามกฎหมายคุ้มครองแรงงาน ในกรณีนี้นายจ้าง (ธนาคาร) สามารถทำการเก็บรวบรวมข้อมูลอ่อนไหวได้ ในที่นี้คือข้อมูลสุขภาพที่ระบุอยู่ในใบรับรองแพทย์โดยไม่ต้องขอความยินยอม เนื่องจากเป็นกรณียกเว้นไม่ต้องขอความยินยอมในการประมวลผลข้อมูลอ่อนไหว หากการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการคุ้มครองแรงงาน

5.5 การประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัวเป็นข้อความหรือรายละเอียด ที่ธนาคารจะต้องแสดงกับเจ้าของข้อมูลส่วนบุคคล เพื่ออธิบายเกี่ยวกับรายละเอียดในการประมวลผลข้อมูล ประกาศความเป็นส่วนตัวจะช่วยเพิ่มความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคลของธนาคารเอง ตามหลักการการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส Principle 1 : (" Lawfulness, Fairness, and Transparency") ซึ่งเป็นหลักการที่สำคัญสำหรับเรื่องนี้ ซึ่งจะช่วยให้เจ้าของข้อมูลส่วนบุคคลมั่นใจได้ว่า ธนาคารปฏิบัติอย่างไรกับข้อมูลของตน อีกทั้งเพื่อให้ความเชื่อมั่นแก่เจ้าของข้อมูลส่วนบุคคล ว่าข้อมูลที่ตนได้ให้ไว้กับธนาคารหรือที่ธนาคารได้มาจากแหล่งอื่นนั้น จะไม่ถูกนำไปประมวลผลนอกเหนือจากรายละเอียดตามที่ระบุไว้ในประกาศความเป็นส่วนตัว ดังนั้น ธนาคารจึงต้องอธิบายในรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลทั้งหมด ในภาษาที่เข้าใจได้ง่าย เพื่อเป็นการแจ้งให้กับเจ้าของข้อมูลส่วนบุคคลทราบว่าธนาคารกำลังเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้างของลูกค้า เพื่อบรรลุวัตถุประสงค์อะไร และมีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ประเภทของบุคคลหรือหน่วยงานใดบ้าง และจะทำการเก็บข้อมูลไว้เป็นระยะเวลาเท่าใด รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นต้น นอกจากนั้นธนาคารจะต้องทำการแจ้งประกาศความเป็นส่วนตัวแก่ลูกค้า ด้วยวิธีการหรือช่องทางที่ลูกค้าสามารถเข้าถึงได้ง่าย ซึ่งอาจทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ธนาคารจะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลก่อน หรือขณะเก็บรวบรวม เกี่ยวกับรายละเอียดในการประมวลผลข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว ซึ่งจะต้องแสดงรายละเอียดของประกาศความเป็นส่วนตัวในหัวข้อดังต่อไปนี้

1. ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) ให้ธนาคารแจ้งรายละเอียดการติดต่อธนาคารและรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (หากมี) ให้ชัดเจนเพื่อให้เจ้าของข้อมูลส่วนบุคคลติดต่อได้ เช่น ชื่อบริษัท สถานที่ติดต่อ ช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล
2. ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม : ให้ธนาคารแสดงรายการข้อมูลส่วนบุคคลที่ต้องการเก็บรวบรวม ใช้ และเปิดเผยเพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ให้เจ้าของข้อมูลส่วนบุคคลทราบ
3. แหล่งที่มาของข้อมูล : ให้ธนาคารแสดงรายละเอียดการได้มาของข้อมูล อันได้แก่ ทำการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง หรือการเก็บรวบรวมข้อมูลจากแหล่งที่อื่นด้วย เช่น จากการที่ธนาคารสามารถเข้าถึงข้อมูลจากแหล่งอื่นที่น่าเชื่อถือ เช่น หน่วยงานราชการ บริษัทในกลุ่มธุรกิจทางการเงินของธนาคาร และ/หรือบริษัทพันธมิตรของธนาคาร หรือที่ปรึกษาของธนาคาร

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

4. ข้อความแสดงวัตถุประสงค์ : เป็นการบอกวัตถุประสงค์ของการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล ซึ่งในประกาศความเป็นส่วนตัวจะต้องมีการระบุวัตถุประสงค์ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลไว้อย่างชัดเจน และครอบคลุมทุกวัตถุประสงค์ของกิจกรรมการประมวลผล ธนาคารไม่ควรกล่าวอย่างกว้างเกินไป หรือกล่าวอย่างคลุมเครือ เพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจว่าข้อมูลส่วนบุคคลจะถูกนำไปประมวลผลอย่างไร
5. ฐานการประมวลผลข้อมูลส่วนบุคคล : ธนาคารต้องระบุฐานในการประมวลผลข้อมูลโดยพิจารณาฐานที่ใช้ในการประมวลผลตามหัวข้อ “5.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล” โดยธนาคารจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง และธนาคารจะต้องแจ้งให้ทราบถึงความจำเป็นที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นที่ต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา และแจ้งผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล โดยระบุรายละเอียดไว้ในฐานการประมวลผลตามกฎหมาย
6. คำอธิบายการประมวลผลข้อมูลส่วนบุคคล : ธนาคารทำการแจ้งรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล อันได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคล การใช้ข้อมูล และประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผย โดยให้ระบุอย่างชัดเจน ซึ่งอาจระบุรวมไว้กับวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าและเหตุผลในการประมวลผลข้อมูลตามวัตถุประสงค์
7. ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล : ธนาคารต้องทำการระบุระยะเวลาในการเก็บรักษาข้อมูลไว้อย่างชัดเจน ตามเกณฑ์ที่ธนาคารใช้ในการพิจารณาระยะเวลาในการเก็บข้อมูลส่วนบุคคล เช่น ภาระผูกพันตามกฎหมายที่ต้องเก็บตามระยะเวลาที่กำหนด อาทิ กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยสถาบันการเงิน กฎหมายว่าด้วยภาษีอากร กฎหมายว่าด้วยการบัญชี ซึ่งธนาคารอาจระบุวิธีการทำลายข้อมูลส่วนบุคคล หรือการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้เมื่อสิ้นสุดระยะเวลาในการเก็บข้อมูล
8. สิทธิของเจ้าของข้อมูลส่วนบุคคล : ธนาคารต้องอธิบายสิทธิของเจ้าของข้อมูลส่วนบุคคลทั้งหมดอย่างชัดเจน และรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ทำหน้าที่รับผิดชอบต่อการจัดการข้อมูลส่วนบุคคลเพื่อให้เจ้าของข้อมูลส่วนบุคคลทำการร้องขอได้ ผู้อ่านสามารถดูรายละเอียดเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ในหัวข้อ “10. แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล”

5.5.1 ตัวอย่างประกาศความเป็นส่วนตัว/นโยบายความเป็นส่วนตัว (Privacy Notice or Privacy Policy)

<u>นโยบายความเป็นส่วนตัว (Privacy Notice)</u>

ธนาคาร ABC จำกัด (“ธนาคาร”) มุ่งเน้นที่จะให้บริการที่ดีที่สุดให้แก่ลูกค้าคนสำคัญของธนาคาร ซึ่งการได้รับความไว้วางใจและความเชื่อมั่นจากท่านในฐานะลูกค้าของธนาคาร (“ลูกค้า”) เป็นสิ่งที่สำคัญอย่างยิ่ง ธนาคารมีความตระหนักถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า ธนาคารจึงมีระบบในการรักษาความปลอดภัยของข้อมูล และขั้นตอนการดำเนินงานที่รัดกุม อีกทั้งมาตรการในการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง เปิดเผย นำไปใช้หรือเปลี่ยนแปลงข้อมูลโดยมิได้รับอนุญาต ดังนั้นธนาคารจึงจัดทำนโยบายฉบับนี้ขึ้นเพื่อชี้แจง รายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ระยะเวลาในการเก็บข้อมูล การทำลายข้อมูล อีกทั้งสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งลูกค้าสามารถศึกษารายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลได้ดังต่อไปนี้

1. ข้อมูลที่ธนาคารทำการเก็บรวบรวม ใช้ หรือเปิดเผย และแหล่งที่มาของข้อมูล ธนาคารทำการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน อันได้แก่

1.1 ข้อมูลส่วนบุคคลทั่วไปที่เป็นข้อมูลแสดงตัวตนของลูกค้า (Identity Data) ซึ่งหมายถึงข้อมูลที่เกี่ยวกับบุคคลธรรมดาที่ทำให้สามารถระบุตัวตนลูกค้ารายนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ/นามสกุล เลขประจำตัวประชาชน เลขหนังสือเดินทาง วัน/เดือน/ปีเกิด รวมถึงข้อมูลอ่อนไหว เช่น ข้อมูลชีวภาพ (ลายนิ้วมือ ข้อมูลใบหน้า) ข้อมูลสุขภาพ เป็นต้น

1.2 ข้อมูลติดต่อของลูกค้า (Contact Data) เช่น ที่อยู่ อีเมล หมายเลขโทรศัพท์

1.3 ข้อมูลทางการเงินหรือข้อมูลการทำธุรกรรมของลูกค้ากับธนาคาร (Financial and Transaction Data) เช่น หมายเลขบัญชีเงินฝาก/เงินลงทุน หมายเลขบัตรเครดิต หมายเลขบัตรเดบิต หรือ รายงานข้อมูลการเบิก/ถอนเงินในบัญชี ข้อมูลรายได้ รายจ่าย ยอดเงินฝากที่มีกับธนาคาร ประวัติสินเชื่อที่มีอยู่กับธนาคาร หรือข้อมูลการชำระหนี้ ข้อมูลจากฐานข้อมูลของกรมบังคับคดี เป็นต้น

1.4 ข้อมูลความชื่นชอบของลูกค้าในการค้นหาข้อมูลจากอินเทอร์เน็ต (Technical and Usage Data) เช่น การค้นหาข้อมูลผลิตภัณฑ์ของธนาคาร (Website Browsing) จากการใช้ Cookies หรือการเชื่อมต่อเว็บไซต์อื่นๆ ที่ลูกค้าเข้าไปค้นหาข้อมูล เป็นต้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

1.5 ข้อมูลการติดต่อกับธนาคาร (Communication Data) เช่น เทปบันทึกในกรณีที่ลูกค้า เข้ามาติดต่อธนาคาร ผ่านทาง Contact Center ซึ่งอาจเป็นภาพหรือเสียง เป็นต้น และไม่ว่าลูกค้าได้ให้ข้อมูลไว้หรือมีอยู่กับธนาคาร หรือ ที่ธนาคารได้รับ หรือ เข้าถึงได้จากแหล่งอื่นที่น่าเชื่อถือ เช่น หน่วยงานราชการ บริษัทในกลุ่มธุรกิจทางการเงินของธนาคาร และ/หรือบริษัทพันธมิตรของธนาคาร หรือที่ปรึกษาของธนาคาร

2. วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า

ทั้งนี้ธนาคารทำการเก็บรวบรวมข้อมูล เพื่อประโยชน์ของท่านในการทำธุรกรรมและ/หรือใช้บริการกับธนาคาร เพื่อปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง และ/หรือเพื่อประโยชน์อื่นใดที่ท่านได้ให้ความยินยอมไว้แก่ธนาคาร โดยธนาคารจะเก็บรักษาข้อมูลของท่านตามมาตรการรักษาความปลอดภัยของธนาคาร ลูกค้าสามารถศึกษารายละเอียดได้ดังต่อไปนี้

2.1 การปฏิบัติตามสัญญาระหว่างลูกค้ากับธนาคาร เช่น การใช้ผลิตภัณฑ์หรือบริการต่างๆ ของลูกค้า การปฏิบัติตามกระบวนการภายในของธนาคาร การทำประกันภัยทรัพย์หลักประกัน การโอนขายกลุ่มลูกหนี้ให้แก่บุคคลอื่น การรับ-ส่งเอกสารติดต่อระหว่างลูกค้ากับธนาคาร การทวงถามให้ลูกค้าชำระหนี้ที่ค้างตามสัญญาสินเชื่อที่มีกับธนาคาร

2.2 การปฏิบัติตามกฎหมาย เช่น การป้องกันและตรวจจับความผิดปรกติของธุรกรรมที่นำไปสู่กิจกรรมที่ผิดกฎหมาย การรายงานข้อมูลของลูกค้าต่อกรมสรรพากร การรายงานข้อมูลส่วนบุคคลต่อหน่วยงานราชการ เช่น ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ กรมสรรพากร หรือ เมื่อได้รับหมายเรียกหมายอายัดจากหน่วยงานราชการ หรือ ศาล เป็นต้น

2.3 ประโยชน์อันชอบด้วยกฎหมายของธนาคาร เช่น

- การป้องกัน รับมือ ลดความเสี่ยงที่อาจเกิดการกระทำที่ผิดกฎหมายต่างๆ ซึ่งรวมถึงการแบ่งปันข้อมูลส่วนบุคคลเพื่อยกระดับมาตรฐานการทำงานของบริษัทในธุรกิจเดียวกันในการป้องกัน รับมือ ลดความเสี่ยงข้างต้น
- การบันทึกภาพผู้ที่มาติดต่อทำธุรกรรมกับสำนักงานหรือสาขาของธนาคารลงบน CCTV รวมถึง การแลกบัตรก่อนเข้าอาคาร เพื่อการรักษาความปลอดภัยภายในบริเวณอาคารของธนาคาร
- การบริหารความเสี่ยง/การกำกับตรวจสอบ/การบริหารจัดการภายในองค์กร รวมถึงการส่งต่อไปยังบริษัทในเครือกิจการและ/หรือกลุ่มธุรกิจทางการเงินเพื่อการดังกล่าว ภายใต้นโยบายในการคุ้มครองข้อมูล

ส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

- การตรวจสอบการรับส่งอีเมลหรือการใช้อินเทอร์เน็ตของพนักงานกับลูกค้า เพื่อป้องกันการเปิดเผยข้อมูลลับของธนาคารต่อบุคคลภายนอก
- การวิเคราะห์ข้อมูลเพื่อใช้ในการนำเสนอผลิตภัณฑ์ในประเภทเดียวกันกับที่ลูกค้ามีอยู่กับธนาคารและผลิตภัณฑ์อื่นของธนาคารให้แก่ลูกค้า อย่างเหมาะสมกับความต้องการของลูกค้าและ/หรือในการทำวิจัยทางการตลาด เพื่อพัฒนาผลิตภัณฑ์ของธนาคาร
- การรักษาความสัมพันธ์กับลูกค้า เช่น การจัดการข้อร้องเรียน การเสนอสิทธิประโยชน์พิเศษโดยไม่มีวัตถุประสงค์ทางการตลาดให้แก่ลูกค้า เป็นต้น

ทั้งนี้ หากลูกค้าไม่ให้ข้อมูลส่วนบุคคลกับเราอาจส่งผลกระทบต่อลูกค้าในการไม่ได้รับการให้ผลิตภัณฑ์/บริการ ไม่ได้รับความสะดวก หรือไม่ได้รับการปฏิบัติตามสัญญาและลูกค้าอาจได้รับความเสียหาย/เสียโอกาสและอาจส่งผลกระทบต่อการปฏิบัติตามกฎหมายใดๆ ที่ลูกค้าหรือธนาคารต้องปฏิบัติตาม และอาจมีบทกำหนดโทษที่เกี่ยวข้อง

3. การเปิดเผยข้อมูลส่วนบุคคล

ธนาคารจะทำการเปิดเผยข้อมูลให้แก่บุคคลภายนอกในกรณีดังต่อไปนี้

- เป็นการเปิดเผยข้อมูลส่วนบุคคลให้แก่ บริษัทในกลุ่มธุรกิจทางการเงินได้แก่ บริษัท abc ประกันภัย จำกัด, บริษัท abc บริหารสินทรัพย์ จำกัด, บริษัท abc หลักทรัพย์จำกัด และ พันธมิตรทางธุรกิจของธนาคาร ได้แก่ บริษัท XYZbank จำกัด
- เปิดเผยข้อมูลให้แก่ Credit Bureau ที่ธนาคารเป็นสมาชิก
- เปิดเผยข้อมูลให้แก่บุคคลภายนอกตามที่ธนาคารได้รับความยินยอมจากลูกค้า
- เปิดเผยข้อมูลเพื่อการทำธุรกรรม และ/หรือ การใช้บริการตามความประสงค์ของลูกค้า
- เปิดเผยแก่ผู้บริการภายนอก (Outsource/Service Provider) ที่ธนาคารเป็นคู่สัญญา ทั้งในประเทศไทยและต่างประเทศ เช่น ผู้ให้บริการ Cloud Computing บริษัทรับจ้างทำกิจกรรมทางการตลาด บริษัทรับจ้างทำวิจัยให้แก่ธนาคาร บริษัทรับจ้างพัฒนาเทคโนโลยีสารสนเทศให้แก่ธนาคาร
- เปิดเผยให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแล เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ เช่น ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสรรพากร สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ศาล รวมทั้งผู้สอบบัญชี

4. สิทธิของลูกค้าเกี่ยวกับข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ธนาคารคำนึงถึงสิทธิส่วนบุคคลของลูกค้า ซึ่งสิทธิของลูกค้าในข้อนี้เป็นสิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ลูกค้าควรทราบ ได้แก่

4.1 สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”)

ลูกค้ามีสิทธิขอเพิกถอนความยินยอมที่จะให้ไว้กับธนาคารในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าเมื่อใดก็ได้ เว้นแต่การเพิกถอนความยินยอมจะมีข้อจำกัดโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่ลูกค้า เช่น ลูกค้ายังมีการใช้บริการ/ผลิตภัณฑ์จากธนาคาร หรือลูกค้ายังมีภาระหนี้/ภาระผูกพันอยู่กับธนาคาร เป็นต้น

4.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”)

ลูกค้ามีสิทธิขอทราบและขอรับสำเนาข้อมูลส่วนบุคคลของลูกค้าซึ่งอยู่ในความรับผิดชอบของธนาคาร หรือ ขอให้ธนาคารเปิดเผยการได้มาซึ่งข้อมูลที่ลูกค้าไม่ได้ให้ความยินยอมได้

4.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)

ลูกค้ามีสิทธิขอให้ธนาคารดำเนินการแก้ไขเพื่อให้ข้อมูลถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

4.4 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)

ลูกค้ามีสิทธิขอรับข้อมูลที่เกี่ยวกับลูกค้าจากธนาคาร ในกรณีที่ธนาคารได้ทำให้ข้อมูลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือ ใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ รวมทั้ง (ก) มีสิทธิขอให้ธนาคารส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น เมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ หรือ (ข) ขอรับข้อมูลที่ธนาคารส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่สภาพทางเทคนิคไม่สามารถทำได้

4.6 สิทธิในการลบข้อมูลส่วนบุคคล (“Right to Erasure” or “Right to be Forgotten”)

ลูกค้ามีสิทธิขอให้ธนาคารลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลว่าเป็นลูกค้าได้ ในกรณีดังนี้

- ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นสำหรับวัตถุประสงค์ในการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคล ทำการถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและธนาคารไม่มีอำนาจตามกฎหมายที่จะทำการประมวลผลได้
- เจ้าของข้อมูลส่วนบุคคล คัดค้านการประมวลผลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

- เป็นการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย
- เจ้าของข้อมูลส่วนบุคคล คัดค้านการประมวลผลข้อมูล (นอกเหนือจากที่เกี่ยวข้องกับการคัดค้านการประมวลผลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง) และธนาคารไม่มีเหตุแห่งการอ้างการประมวลผลโดยประโยชน์อันชอบธรรม

4.7 สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)

ลูกค้ามีสิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลของตน เมื่อเข้าเงื่อนไขดังต่อไปนี้

- การประมวลผลไม่จำเป็นอีกต่อไป แต่การเก็บรักษาข้อมูลส่วนบุคคลยังคงมีความจำเป็นเพื่อการใช้สิทธิเรียกร้องทางกฎหมาย
- เป็นการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลนั้นต้องการห้ามมิให้มีการประมวลผลโดยแทนการลบหรือทำลายข้อมูลส่วนบุคคลของตน
- เมื่ออยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล ตามที่ลูกค้าร้องขอ
- เมื่อธนาคารอยู่ในระหว่างการพิสูจน์ให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า

4.8 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)

ลูกค้ามีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลที่เกี่ยวกับลูกค้า ในกรณีดังนี้

- กรณีที่เป็นการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- กรณีที่เป็นการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่การจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของธนาคาร
- กรณีที่เป็นข้อมูลที่เก็บรวบรวมได้ด้วยเหตุจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของธนาคาร หรือ เหตุจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของธนาคาร เว้นแต่ธนาคารแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า หรือ เป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือ การใช้สิทธิเรียกร้องตามกฎหมาย หรือ การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5. มาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

ธนาคารมีการกำหนดนโยบาย แนวปฏิบัติและมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้า ทั้งมาตรการในการบริหารจัดการ (Organizational Measure) และมาตรการเชิงเทคนิค (Technical Measure) เพื่อป้องกันการเข้าถึงข้อมูลของท่านโดยมิได้รับอนุญาตหรือการละเมิดข้อมูลส่วนบุคคล เช่น ระบบสารสนเทศในการรักษาความปลอดภัยที่เข้มงวด นโยบายการรักษาข้อมูลความลับของลูกค้า เป็นต้น และธนาคารได้มีการปรับปรุงนโยบาย แนวปฏิบัติและมาตรฐานขั้นต่ำดังกล่าวเป็นระยะๆ ตามเกณฑ์ที่กฎหมายกำหนด

นอกจากนี้ พนักงาน ลูกจ้าง และผู้ให้บริการภายนอกของธนาคารก็มีหน้าที่ต้องรักษาความลับของข้อมูลส่วนบุคคลของลูกค้าตามสัญญารักษาความลับที่ได้ลงนามไว้กับธนาคาร และในกรณีที่ธนาคารมีความจำเป็นต้องส่ง หรือ โอนข้อมูลส่วนบุคคลของลูกค้าไปต่างประเทศที่มีมาตรฐานการจัดการข้อมูลส่วนบุคคลต่ำกว่าประเทศไทย

6.ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ในกรณีที่ลูกค้ายุติความสัมพันธ์ทางธุรกิจกับธนาคารไปแล้ว ธนาคารจะจัดเก็บข้อมูลส่วนบุคคลของลูกค้าตามที่กฎหมายกำหนดและตามนโยบาย แนวปฏิบัติต่างๆ ในเรื่องการจัดเก็บ ทำลายเอกสารต่างๆ ของธนาคาร เช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงินกำหนดให้จัดเก็บไว้อย่างน้อย 10 ปี เป็นต้น และเมื่อสิ้นสุดระยะเวลาในการเก็บแล้วธนาคารจะทำลายข้อมูลส่วนบุคคลดังกล่าว

7. ข้อมูลการติดต่อธนาคาร

หากลูกค้าต้องการติดต่อหรือมีข้อสงสัยหรือต้องการสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล การใช้สิทธิของลูกค้า หรือมีข้อร้องเรียนใดๆ ลูกค้าสามารถติดต่อธนาคารได้ดังช่องทางต่อไปนี้

- ศูนย์บริการลูกค้า (Contact Center) โทร 1234
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเรา (Data Protection Officer) (นาย ข. email: dpo@abcbank.com)
- เว็บไซต์ของธนาคาร www.abcbank.com
- สถานที่ติดต่อ (ระบุที่อยู่ในการติดต่อ)

6. การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage and Data Disclosure)

หลังจากที่ธนาคารทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลแล้ว ธนาคารอาจมีความจำเป็นที่ต้องใช้หรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นที่เกี่ยวข้อง ซึ่งการเปิดเผยข้อมูล ธนาคารสามารถทำได้เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูล หรือการเปิดเผยมีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว หรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานใด ซึ่งโดยหลักการแล้วหากต้องมีการเปิดเผยข้อมูลส่วนบุคคล ธนาคารต้องมีการแจ้งกับเจ้าของข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) ซึ่งจะต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล ถึงความจำเป็นในการใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์ใด อีกทั้งต้องระบุประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผยอย่างชัดเจน

ตัวอย่าง แนวปฏิบัติในการใช้หรือเปิดเผยข้อมูลไปยังบุคคลหรือหน่วยงานต่าง ๆ

ตัวอย่าง แนวปฏิบัติในการเปิดเผยข้อมูลเพื่อการทำธุรกรรม และ/หรือ การใช้บริการตามความประสงค์ของลูกค้า

ตัวอย่าง 1 ธนาคารทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า เพื่อวัตถุประสงค์ในการสมัครบัตรเครดิตให้กับลูกค้า ในการดำเนินการขออนุมัติการเปิดบัตรเครดิตนั้น ธนาคารมีความจำเป็นที่จะต้องทำการเปิดเผยข้อมูลไปยังบริษัทแม่ที่อยู่ในประเทศหรือต่างประเทศเพื่อทำการอนุมัติบัตรเครดิต การเปิดเผยในกรณีนี้ ให้เป็นไปตามนโยบายการเปิดเผยข้อมูลของกลุ่มเครือธนาคารเอง

ตัวอย่าง แนวปฏิบัติในการเปิดเผยข้อมูลแก่ผู้บริการภายนอก (Outsource/Service Provider) ที่ธนาคารเป็นคู่สัญญา ทั้งในประเทศไทยและต่างประเทศ

ตัวอย่าง 1 ธนาคารทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าไปยังผู้ให้บริการภายนอก เพื่อวัตถุประสงค์ในการพัฒนาเทคโนโลยีสารสนเทศของธนาคาร ธนาคารอาจมีการเปิดเผยไปยังบุคคลภายนอก (Outsource) ที่ธนาคารทำการจัดจ้าง เช่น ผู้ให้บริการ Cloud Computing เพื่อเก็บรักษาข้อมูลส่วนบุคคลไว้ในระบบคลาวด์ ธนาคารควรที่จะทำสัญญาระหว่างธนาคารและผู้ให้บริการภายนอก (Data Processing Agreement) เพื่อเป็นการกำหนดอย่างชัดเจนว่า บริษัทที่ธนาคารทำการจัดจ้างผู้ซึ่งทำหน้าที่เป็นผู้ประมวลผลข้อมูลนั้นจะประมวลผลข้อมูลส่วนบุคคลเฉพาะตามข้อตกลงที่ทำไว้กับธนาคาร ไม่ประมวลผลนอกเหนือไปกว่าที่กำหนดไว้ นอกจากนั้นธนาคารจะต้องมั่นใจว่าบริษัทที่ธนาคารจัดจ้าง มีมาตรการในการรักษาความปลอดภัยที่เพียงพอ เพื่อให้แน่ใจว่าข้อมูลที่ถูกเปิดเผยจะได้รับการรักษาความปลอดภัยอย่างเหมาะสม

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตัวอย่าง 2 ในกรณีที่ลูกค้าเงินกู้ของธนาคารผิดนัดชำระหนี้กับธนาคารเกินระยะเวลาที่กำหนด ธนาคารทำการจัดจ้างตัวแทนในการเรียกเก็บหนี้ เพื่อเรียกเก็บหนี้ที่ค้างชำระ/จัดจ้างทนายความ เพื่อยื่นฟ้องลูกหนี้ที่ค้างชำระ ธนาคารสามารถเปิดเผยข้อมูลของลูกหนี้ ให้กับตัวแทนในการเรียกเก็บหนี้หรือทนายความ เพื่อเรียกเก็บหนี้ดังกล่าวได้ภายใต้สัญญาที่ทำร่วมกัน (Data Processing Agreement) เพื่อกำหนดอย่างชัดเจนว่า ตัวแทนที่ธนาคารทำการจัดจ้างผู้ซึ่งทำหน้าที่เป็นผู้ประมวลผลข้อมูลนั้นจะประมวลผลข้อมูลส่วนบุคคลเฉพาะตามข้อตกลงที่ทำไว้กับธนาคาร ไม่ประมวลผลนอกเหนือไปกว่าที่กำหนดไว้ สำหรับการทวงถามหนี้ให้เป็นไปตามเกณฑ์ของพระราชบัญญัติการทวงถามหนี้

ตัวอย่าง แนวปฏิบัติในการเปิดเผยข้อมูลแก่ผู้บริการภายนอก (Outsource/Service Provider) ที่ธนาคารเป็นคู่สัญญา ทั้งในประเทศไทยและต่างประเทศ

ตัวอย่าง 3 กรณีลูกค้าธนาคารโอนเงินไปต่างประเทศ ซึ่งธนาคารจะต้องมีการส่งข้อมูลให้แก่ผู้บริการ Switching ผู้ให้บริการระบบการชำระเงินระหว่างประเทศที่อยู่ในต่างประเทศและธนาคารในต่างประเทศ โดยในกรณีดังกล่าวข้างต้นธนาคารสามารถอ้างอิงตามมาตรา 28 (3) ซึ่งเป็นการปฏิบัติตามสัญญาระหว่างธนาคารและเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างที่ 4 กรณีที่ธนาคารเปิดเผยข้อมูลส่วนบุคคลของลูกค้าให้แก่ผู้บริการภายนอกซึ่งอยู่ในประเทศปลายทางที่ไม่มีมาตราฐานการคุ้มครองข้อมูลส่วนบุคคลเพียงพอ เพื่อวัตถุประสงค์ในการทำ Data Analytic เพื่อพัฒนาผลิตภัณฑ์/บริการของธนาคาร หรือการนำเสนอผลิตภัณฑ์/บริการของธนาคาร หรือการนำเสนอผลิตภัณฑ์/บริการแก่ลูกค้า โดยในกรณีดังกล่าวข้างต้นธนาคารสามารถอ้างอิงมาตรา 28 (4) ซึ่งเป็นการทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง แนวปฏิบัติในการเปิดเผยข้อมูลให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแล เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ

ตัวอย่าง 1 เพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงานรัฐ ธนาคารสามารถเปิดเผยข้อมูลให้แก่หน่วยงานราชการหรือหน่วยงานกำกับดูแลได้ เช่น ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสรรพากร สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ศาล รวมทั้งผู้สอบบัญชี บริษัทข้อมูลเครดิต เป็นต้น

6.1 แนวปฏิบัติในการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการในประเทศ

โดยปกติธุรกิจของธนาคาร อาจมีโครงสร้างการถือหุ้น โดยมีบริษัทแม่หรือมีบริษัท Holding Company ที่ถือหุ้นของบริษัทในเครืออยู่ ธนาคารจึงอาจมีความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลระหว่างกันภายในกลุ่มบริษัทในเครือที่อยู่ในประเทศ เช่น เพื่อวัตถุประสงค์ในการให้บริการแก่ลูกค้า เพื่อการบริหารความเสี่ยงภายในกลุ่มเครือ เป็นต้น ให้ธนาคารทำการแจ้งรายละเอียดแก่เจ้าของข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) โดยระบุถึงความจำเป็นในการเปิดเผยข้อมูลภายในบริษัทในเครือ และประเภทของบุคคลหรือหน่วยงานด้วย สำหรับฐานตามกฎหมายในการเปิดเผยข้อมูลส่วนบุคคลนั้น ขึ้นอยู่กับกิจกรรมการประมวลผลข้อมูล โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “5.2 แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล”

อย่างไรก็ตามแม้ว่าจะเป็นการเปิดเผยข้อมูลระหว่างบริษัทในเครือเดียวกัน ธนาคารควรจะต้องจัดทำนโยบายในการเปิดเผยข้อมูลระหว่างเครือกิจการ เพื่อให้บริษัทในเครือมีแนวปฏิบัติเป็นไปในทิศทางเดียวกัน เป็นมาตรฐานเดียวกัน และพนักงานทุกคนจะต้องทราบและปฏิบัติตาม ซึ่งนโยบายควรมีการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลอย่างเหมาะสม ให้เพียงเฉพาะบุคคลหรือแผนกที่จำเป็นต้องใช้ในการประมวลผลตามวัตถุประสงค์เท่านั้น ภายใต้หลักการ “Need to know” และ “Need to use” เพื่อเป็นการป้องกันการเข้าถึง เปลี่ยนแปลง แก้ไขข้อมูลโดยมิชอบ หรืออาจถูกนำไปใช้นอกเหนือจากวัตถุประสงค์ในการประมวลผลข้อมูล มีมาตรการในรักษาความปลอดภัยของข้อมูล ทั้งในเชิงบริหารจัดการและเชิงเทคนิค และมีการตรวจสอบ ติดตามผลการปฏิบัติตามนโยบายหรือแนวปฏิบัติการปฏิบัติงานอย่างสม่ำเสมอ

6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Cross-border data transfer)

ธนาคารอาจมีความจำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามประกาศกำหนด

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ อย่างไรก็ตาม ปัจจุบันคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้มีการกำหนดรายละเอียดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ แนวปฏิบัติฉบับนี้จึงนำหลักเกณฑ์ของ GDPR มาเป็นแนวปฏิบัติในกับกลุ่มธนาคารไทย

ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ ธนาคารสามารถทำในกรณีดังต่อไปนี้

6.2.1 ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

แนวทางการพิจารณาความเพียงพอของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่รับโอนข้อมูลส่วนบุคคล (Adequacy of the Level of Protection) สามารถพิจารณาได้โดย

1) พิจารณาจากกฎหมายของประเทศดังกล่าว ว่ามีการคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐาน จากกฎหมายที่เกี่ยวข้องทั้งในภาพรวมหรือกฎหมายเฉพาะ รวมถึงการรักษาความมั่นคงของชาติ กฎหมายอาญา การเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานรัฐ การบังคับใช้กฎหมาย กฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล กฎเกณฑ์ของผู้ประกอบวิชาชีพ มาตรการในการรักษาความปลอดภัยของข้อมูล กฎเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ ความมีประสิทธิภาพในการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลหากข้อมูลส่วนบุคคลที่ถูกโอนนั้นถูกละเมิด
2) การมีอยู่และการทำงานขององค์กร/หน่วยงานอิสระในต่างประเทศหรือหน่วยงานระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล ว่ามีอำนาจหน้าที่ในการบังคับใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และอำนาจหน้าที่ในการให้ความช่วยเหลือเจ้าของข้อมูลส่วนบุคคล ในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและอำนาจหน้าที่ในการร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรไทย
3) ข้อผูกพันระดับนานาชาติของประเทศหรือองค์การระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล เกิดจากการที่ประเทศหรือองค์กรระหว่างประเทศผู้รับโอนได้เข้าผูกพันทางกฎหมาย โดยเฉพาะที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือ การเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

ตัวอย่างการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ธนาคาร A มีความประสงค์ที่จะจ้าง บริษัท B ซึ่งเป็นบริษัทที่ให้บริการระบบคลาวด์ (Cloud Service Provider) โดยมีสาขาในประเทศไทย ซึ่งมีศูนย์จัดเก็บข้อมูลที่ประเทศญี่ปุ่นและฮ่องกง หากธนาคาร A ต้องการจะใช้งานระบบคลาวด์ของบริษัท B ธนาคาร A จะต้องมั่นใจว่า ในการเก็บข้อมูลที่ศูนย์ข้อมูลหรือการประมวลผลย่อยของข้อมูลส่วนบุคคลที่จะเกิดขึ้นในประเทศที่ญี่ปุ่นและฮ่องกง ประเทศดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เทียบเท่าหรือมากกว่ากฎหมายของประเทศไทยหรือไม่

หากมีการละเมิดข้อมูลเกิดขึ้นในขณะที่ข้อมูลส่วนบุคคลอยู่ในความดูแลของบริษัท B ในการพิจารณาว่าธนาคาร A มีความผิดจากการละเมิดข้อมูลส่วนบุคคลหรือไม่ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลล อาจมีการพิจารณาถึงการตรวจสอบมาตรฐานของประเทศที่รับโอนข้อมูลส่วนบุคคลของธนาคาร A (Due Diligence) เนื่องจากการพิจารณาความพอเพียงของมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง ถือเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่างการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ในกรณีที่มีความจำเป็นเพื่อการปฏิบัติตามสัญญา ที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น ธนาคารสามารถทำได้ภายใต้มาตรา 28(3)

6.2.2 กรณีที่ได้รับการยกเว้นตามกฎหมาย

ธนาคารสามารถโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศได้ แม้ว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางไม่เพียงพอหากเข้ากรณียกเว้นตามกฎหมายดังต่อไปนี้

1) เป็นการปฏิบัติตามกฎหมาย
2) ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยธนาคารได้แจ้งให้เจ้าของข้อมูลส่วนบุคคล ทราบถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือ องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

6.2.3 กรณีที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Transfers Subject to Appropriate Safeguards)

1) ธนาคารมี "นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ" (Binding Corporate Rules) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคลแล้ว ในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน นั้นสามารถทำได้ตามข้อกำหนดในนโยบายดังกล่าว โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ "6.3 แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ"
2) กรณีที่คณะกรรมการมาตรการคุ้มครองข้อมูลส่วนบุคคลยังไม่มีประกาศหลักเกณฑ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ ธนาคารสามารถใช้มาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมอื่น ๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตามข้อกำหนดของ GDPR ได้แก่
   2.1) ข้อสัญญาที่เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Standard Data Protection Clauses) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ
   2.2) หลักปฏิบัติด้านจรรยาบรรณ (Code of Conduct) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ หลักปฏิบัติด้านจรรยาบรรณ ดังกล่าวต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
   2.3) คำรับรองเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Certification Mechanism) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ ซึ่งคำรับรองดังกล่าวต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการ

คุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

2.4) ข้อสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Contractual Clauses) ผู้ประมวลผลหรือผู้รับข้อมูลส่วนบุคคลในประเทศปลายทางที่ได้รับอนุมัติจาก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ

2.5) ข้อบัญญัติเพิ่มเติม ในข้อตกลงการบริหารงานระหว่างหน่วยงานสาธารณะ (Provision to be Inserted into Administrative Arrangements Between Public Authorities) ที่ได้รับอนุมัติจาก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ ซึ่งมีผลบังคับใช้ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

6.3 แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ

1) จัดให้มี “นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ” (Binding Corporate Rules) เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือประกอบธุรกิจร่วมกัน นโยบายดังกล่าวเป็นการกำหนดแนวทางในการปฏิบัติของกลุ่มเครือกิจการในการโอนข้อมูลระหว่างกัน ซึ่งจะต้องมีการบังคับใช้กับทุกบริษัทในเครือ หากนโยบายดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงานคุ้มครองข้อมูลส่วนบุคคลแล้ว การส่งหรือโอนข้อมูลไปยังต่างประเทศที่เป็นไปตามนโยบายนั้นสามารถกระทำได้ อย่างไรก็ตาม ปัจจุบันคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมิได้มีการกำหนดรายละเอียดหลักเกณฑ์ในการตรวจสอบนโยบายดังกล่าว แนวปฏิบัติฉบับนี้จึงนำหลักเกณฑ์ Binding Corporate Rules ของ GDPR มาเป็นแนวทางในการกำหนดนโยบายดังกล่าว ซึ่งมีสาระสำคัญของนโยบายดังต่อไปนี้

- กำหนดให้นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการมีสภาพบังคับตามกฎหมายและให้มีผลบังคับใช้กับทุกสมาชิกของบริษัทในเครือ รวมถึงลูกจ้างและพนักงานของสมาชิก
- กำหนดให้นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
  <u>และควรมีเนื้อหาของนโยบายที่ครอบคลุมอย่างน้อยดังหัวข้อต่อไปนี้</u>
- โครงสร้างและรายละเอียดการติดต่อของแต่ละสมาชิกของกลุ่มกิจการหรือกลุ่มบริษัทที่มีส่วนร่วมในการประกอบกิจการร่วมกัน
- อธิบายขอบเขตของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทในเครือ รวมถึง สภาพของการส่งหรือโอนข้อมูล ประเภทเจ้าของข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

- การใช้หลักการในการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง การประมวลผลข้อมูลตามวัตถุประสงค์ การเก็บรวบรวมข้อมูลเฉพาะเท่าที่จำเป็น ระยะเวลาในการเก็บ การรักษาความปลอดภัยของข้อมูล ฐานการประมวลผลข้อมูลตามกฎหมาย เป็นต้น
- สิทธิของเจ้าของข้อมูลส่วนบุคคลและวิธีการหรือช่องทางในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หรือบุคคลที่ทำหน้าที่รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสมาชิกของกลุ่มเครือกิจการ อีกทั้ง การติดตามการฝึกอบรมให้ความรู้แก่พนักงาน การจัดการกับข้อร้องเรียน
- กลไกในการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มเครือกิจการ เพื่อให้มั่นใจว่ามีการตรวจสอบและประเมินการปฏิบัติตาม นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ รวมทั้งตรวจสอบการปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การดำเนินการตามเรื่องร้องขอของเจ้าของข้อมูลส่วนบุคคล การดำเนินการแก้ไขเมื่อได้รับเรื่องร้องเรียน
- การอบรมให้ความรู้แก่พนักงานที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้
- มาตรการรับเรื่องร้องเรียนที่เหมาะสม
- กำหนดหน้าที่ในการให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล

2) ธนาคารควรติดตามความเหมาะสมของการใช้งานข้อมูลส่วนบุคคลว่ามีการใช้ข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดในนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการหรือไม่ และมีการตรวจสอบให้แน่ใจว่ามีการทำลายข้อมูลส่วนบุคคลอย่างเหมาะสมหลังจากที่สิ้นสุดความจำเป็นในการใช้งานหรือตามระยะเวลาการเก็บข้อมูลส่วนบุคคลที่กำหนดในนโยบายดังกล่าว

6.4 การประมวลผลข้อมูลเพื่อวัตถุประสงค์เฉพาะ

6.4.1 การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง (Direct Marketing)

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง ซึ่งทำผ่านช่องทางต่าง ๆ เช่น การโทรติดต่อ ส่งการอีเมล ข้อความSMS โทรสาร หรืออื่นๆ เพื่อนำเสนอข้อมูลเกี่ยวกับผลิตภัณฑ์ของธนาคารแก่ลูกค้า สามารถแบ่งได้เป็นหลากหลายกรณีดังต่อไปนี้

Scenario	แนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคล
1. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทอื่นของธนาคาร	ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม เพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของธนาคารให้

	เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำเสนอผลิตภัณฑ์อื่นของธนาคาร
2. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกัน/ ใกล้เคียงกับที่ลูกค้ามีอยู่ของธนาคาร	ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม เพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของธนาคารให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียงกับที่ลูกค้ามีอยู่กับธนาคาร
3. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทอื่น ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ (กรณีที่ธนาคารมีการเปิดเผยข้อมูลส่วนบุคคล)	ธนาคารจะต้องทำการขอความยินยอมจากลูกค้า (ตาม Market Conduct) ในกรณีที่ต้องการเปิดเผยข้อมูลส่วนบุคคลที่ธนาคารมีอยู่ให้กับกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ สำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจของธนาคารให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์อื่นของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ
4. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกัน/ ใกล้เคียงกับที่ลูกค้ามีอยู่ ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ (กรณีที่ธนาคารมีการเปิดเผยข้อมูลส่วนบุคคล)	ธนาคารจะต้องทำการขอความยินยอมจากลูกค้า (ตาม Market Conduct) ในกรณีที่ต้องการเปิดเผยข้อมูลส่วนบุคคลที่ธนาคารมีอยู่ให้กับกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ สำหรับการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจของธนาคารให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่ ขอกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ
5. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์	ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม เพื่อวัตถุประสงค์ในการ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่น ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ (กรณีที่ธนาคารไม่ได้มีการเปิดเผยข้อมูลส่วนบุคคล)	นำเสนอผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจของธนาคารให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น และเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียง รวมถึงผลิตภัณฑ์อื่น ซึ่งผลิตภัณฑ์และบริการที่ธนาคารนำเสนอแก่ลูกค้าจะเป็นผลิตภัณฑ์ที่ธนาคารสามารถนำเสนอได้ภายใต้ใบอนุญาตที่ธนาคารมีอยู่ เช่น กองทุน ประกัน เป็นต้น โดยมิได้มีการเปิดเผยข้อมูลลูกค้าของธนาคารออกไปยังกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจแต่อย่างใด
6. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่นของธนาคาร (ข้อมูลที่เก็บอยู่ก่อน 1 มิ.ย. 2564)	สำหรับข้อมูลที่เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ซึ่งธนาคารทำการเก็บรวบรวมและใช้ข้อมูลตามวัตถุประสงค์เดิม อันได้แก่ เพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียงกับที่ลูกค้ามีอยู่กับธนาคาร รวมทั้งการนำเสนอผลิตภัณฑ์อื่น การประมวลผลดังกล่าวธนาคารสามารถทำได้ภายใต้ฐานประโยชน์อันชอบธรรม
7. การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่นของธนาคาร (ข้อมูลที่เก็บหลัง1 มิ.ย. 2564)	สำหรับข้อมูลที่เก็บรวบรวมไว้หลังวันที่พระราชบัญญัตินี้ใช้บังคับ ซึ่งธนาคารทำการเก็บรวบรวมและใช้ข้อมูลตามวัตถุประสงค์เดิม อันได้แก่ เพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียงกับที่ลูกค้ามีอยู่กับธนาคาร รวมทั้งการนำเสนอผลิตภัณฑ์อื่น ธนาคารสามารถทำได้ภายใต้ฐานประโยชน์อันชอบธรรม
8. Lead Management	กรณีที่ธนาคารได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น เช่น การซื้อข้อมูลลูกค้าจากบริษัทอื่น ข้อมูลดังกล่าวมีรายละเอียดของเจ้าของข้อมูลส่วนบุคคล อันได้แก่ ชื่อนามสกุล รายละเอียดการติดต่อ สำหรับกรณีนี้ธนาคารไม่ต้องขอความยินยอมซ้ำจากเจ้าของข้อมูลส่วนบุคคล แต่ให้บริษัทที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ขอความยินยอมในการเปิดเผยข้อมูลให้กับ

	ธนาคารแต่แรกจากเจ้าของข้อมูลส่วนบุคคล และธนาคารสามารถเก็บรวบรวม ใช้ข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ แต่ทั้งนี้ หากข้อมูลจากแหล่งอื่นดังกล่าวเป็นกรณีที่ธนาคารได้เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลสาธารณะ (เช่น กรมพัฒนาธุรกิจการค้า เฟสบุ๊ค หรือเว็บไซต์สาธารณะอื่น ๆ) ธนาคารจะต้องขอความยินยอมจากลูกค้าในการเก็บ รวบรวมใช้ข้อมูลส่วนบุคคลภายในระยะเวลา 30 วัน หลังจากได้รับข้อมูลดังกล่าว และเมื่อลูกค้าให้ความยินยอมแล้ว ธนาคารจึงจะสามารถใช้ข้อมูลดังกล่าวต่อไปได้

อย่างไรก็ตามกรณีของ Scenario1, Scenario2, Scenario5, Scenario6, Scenario7 ที่ธนาคารไม่ได้ทำการขอความยินยอมจากลูกค้าในรูปแบบ Opt-in Consent แต่ทำการเก็บรวบรวม ใช้ เพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ หรือเพื่อวัตถุประสงค์ทางการตลาด ภายใต้ฐานผลประโยชน์อันชอบธรรม ธนาคารสามารถประมวลผลข้อมูลภายใต้ฐานดังกล่าวได้ หากธนาคารสามารถพิสูจน์ได้ว่าผลประโยชน์อันชอบธรรมของธนาคารหรือของบุคคลที่สามมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล และธนาคารจะต้องแจ้งรายละเอียดหรือวิธีการใด ๆ ที่ให้เจ้าของข้อมูลส่วนบุคคลแจ้งความประสงค์ในการปฏิเสธการรับข่าวสาร (Opt-out) หรือใช้สิทธิคัดค้านการประมวลผลได้ โดยการใช้สิทธินั้นสามารถทำได้ผ่านช่องทางการติดต่อที่ง่ายและสะดวกในการจัดการและการเข้าถึงรวมทั้งมีกระบวนการภายในที่จะสามารถแยกข้อมูลลูกค้าที่จะไม่ประสงค์รับการติดต่อจากธนาคารในการขายผลิตภัณฑ์ได้

7. การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บ (Data Retention)

ธนาคารสามารถทำการเก็บข้อมูลส่วนบุคคล ตามระยะเวลาในการเก็บรักษาเฉพาะเท่าที่จำเป็นตามที่ต้องบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือเก็บตามข้อกำหนดของกฎหมายที่ธนาคารจำเป็นต้องปฏิบัติ เมื่อสิ้นสุดระยะเวลาในการเก็บรักษาแล้วให้ธนาคารดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวมข้อมูลนั้น ๆ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

7.1 แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ธนาคารจะต้องเก็บรักษาข้อมูลส่วนบุคคล เท่าที่จำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูล เพื่อเป็นการปฏิบัติตามหลักการในการคุ้มครองข้อมูลส่วนบุคคล Principle 5 : (“Storage Limitation”) และธนาคารจะต้องมีการระบุระยะเวลาในการเก็บรักษาตามเกณฑ์ที่ธนาคารใช้ในการพิจารณาระยะเวลาในการเก็บข้อมูลส่วนบุคคล เช่น ภาระผูกพันตามกฎหมายที่ต้องเก็บตามระยะเวลาที่กำหนด ไว้ในนโยบายความเป็นส่วนตัวหรือนโยบายคุ้มครองข้อมูลส่วนบุคคล และธนาคารจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา

สำหรับการพิจารณาเพื่อกำหนดระยะเวลาในการเก็บรักษา ควรพิจารณาถึงความจำเป็นของระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อันชอบด้วยกฎหมายในการประมวลผลข้อมูล เนื่องจากความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแต่ละกรณี อาจมีข้อกำหนดของระยะเวลาการเก็บรักษาที่แตกต่างกัน ธนาคารจึงต้องพิจารณาถึงความเหมาะสมของระยะเวลาการเก็บข้อมูลเป็นรายกรณีหรือรายวัตถุประสงค์ในการประมวลผลข้อมูล ซึ่งควรกำหนดไว้ในนโยบายการเก็บรักษา (Retention Policy) หรือแนวปฏิบัติต่าง ๆ อย่างชัดเจน รวมถึงควรระบุวิธีการจัดเก็บ และวิธีการทำลายเอกสารต่าง ๆ เนื่องจากการเก็บข้อมูลส่วนบุคคลเกินความจำเป็นนั้นจะเป็นผลลบต่อธนาคารเอง จะเป็นการเพิ่มความเสี่ยงในการรั่วไหลของข้อมูล อีกทั้งการเก็บข้อมูลจำนวนมากนั้นจะเป็นการเพิ่มค่าใช้จ่ายในการเก็บรักษาข้อมูล

เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม ธนาคารจะต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลนั้น เว้นแต่เป็นไปตามข้อยกเว้นตามกฎหมาย ที่กำหนดให้ธนาคารสามารถเก็บรักษาไว้เพื่อวัตถุประสงค์ดังต่อไปนี้ได้

- การใช้เสรีภาพในการแสดงความคิดเห็น
- การเก็บรักษาไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเกี่ยวกับการศึกษาวิจัยหรือสถิติเพื่อประโยชน์สาธารณะที่มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- การจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ
- การจำเป็นเพื่อปฏิบัติตามกฎหมายให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ หรือประโยชน์สาธารณะด้านสาธารณสุข
- ใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- การใช้ข้อมูลเพื่อฟ้องร้องหรือต่อสู้คดี
- การปฏิบัติตามกฎหมายอื่น

ตัวอย่าง ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์ทางกฎหมาย

ตัวอย่าง 1 ธนาคารจะต้องทำการเก็บรักษาเอกสาร หลักฐานการประกอบการลงบัญชี ตามกฎหมายว่าด้วยการบัญชี (พ.ร.บ.การบัญชี พ.ศ. 2543) ไว้เป็นเวลาไม่น้อยกว่า 5 ปี นับแต่วันที่ปิดบัญชี หรือการเก็บข้อมูลเพื่อการดำเนินคดี

ตัวอย่าง 2 ธนาคารจะต้องเก็บรักษาเอกสารเกี่ยวกับการแสดงตน และเอกสารเกี่ยวกับการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าเป็นเวลา 5 ปีนับแต่วันที่มีการปิดบัญชีหรือยุติความสัมพันธ์กับลูกค้า ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน เว้นแต่จะได้รับแจ้งเป็นหนังสือจากพนักงานเจ้าหน้าที่ให้ปฏิบัติเป็นอย่างอื่น

ตัวอย่าง 3 ธนาคารจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วันก็ได้ แต่มิให้เกินกว่า 2 ปี หรือตามคำสั่งของพนักงานเจ้าหน้าที่ นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตามข้อกำหนดของ พ.ร.บ.ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ตัวอย่าง 4 ธนาคารต้องเก็บและรักษารายงานเกี่ยวกับภาษีมูลค่าเพิ่ม ใบกำกับภาษี และสำเนาใบกำกับภาษี พร้อมทั้งเอกสารประกอบการรายงานหรือเอกสารอื่นที่อธิบดีกรมสรรพากรกำหนดไว้ ณ สถานประกอบการหรือสถานที่อื่นที่อธิบดีกรมสรรพากรกำหนดเป็นเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่ได้ยื่นแบบแสดงรายการภาษีหรือวันทำรายงานแล้วแต่กรณี แต่ไม่เกิน 7 ปี ตามประมวลรัษฎากร

ตัวอย่าง 5 ธนาคารสามารถจัดเก็บข้อมูลส่วนบุคคลของลูกค้าไว้ตามที่พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน ที่กำหนดให้จัดเก็บไว้อย่างน้อย 10 ปี หลังจากที่ลูกค้ายุติความสัมพันธ์ทางธุรกิจกับธนาคารไปแล้ว

ตัวอย่าง 6 ธนาคารทำการเก็บข้อมูลเกี่ยวกับสินเชื่อไว้ 10 ปี หลังจากที่ลูกค้าชำระหนี้เสร็จสิ้น เนื่องจากสอดคล้องกับอายุความ เป็นต้น

8. การลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction)

เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล หรือไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล ธนาคารจะต้องทำการลบหรือทำลายข้อมูลส่วนบุคคล (“การลบ” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใด ๆ) หรือทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ ดังนั้นธนาคารจึงต้องจัดให้มีระบบการตรวจสอบข้อมูลเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อสิ้นสุดความจำเป็น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม เว้นแต่เป็นกรณีที่ได้รับยกเว้นตามกฎหมาย โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ “7.1 แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล”

ธนาคารจึงมีความจำเป็นที่จะต้องมีการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งในการตัดสินใจเลือกใช้วิธีการในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมนั้นจะต้องมีมาตรการเชิงเทคนิคหรือมาตรการเชิงบริหารจัดการ เพื่อเพิ่มมาตรฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น ดำเนินการออกแบบระบบให้รองรับการปฏิบัติงานของธนาคารให้เป็นไปได้อย่างราบรื่น ในขณะเดียวกันก็ต้องมีการคุ้มครองข้อมูลอย่างเหมาะสมและมีประสิทธิภาพ ระบบสามารถทำการตรวจสอบได้ว่าข้อมูลจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น เมื่อสิ้นสุดระยะเวลาในการเก็บ ธนาคารอาจทำข้อมูลให้อยู่ในรูปของข้อมูลนิรนาม (Anonymization) ซึ่งเป็นวิธีการที่จะทำให้ข้อมูลไม่สามารถระบุตัวตนได้ขณะเดียวกันธนาคารจะต้องพิจารณาทั้งต้นทุนในการติดตั้งระบบที่ใช้ในการประมวลผลให้เพียงพอกับผลกระทบ ที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล (Impact) และโอกาสที่อาจเกิดขึ้น (Likelihood) จากการถูกละเมิดข้อมูลส่วนบุคคล

อย่างไรก็ดีหากธนาคารมีการเก็บข้อมูลที่อยู่ในรูปของเอกสาร Hard file การลบหรือทำลายอาจต้องใช้เครื่องทำลายเอกสาร หรือจัดจ้างบริษัททำลายเอกสารเพื่อทำลาย โดยธนาคารต้องมั่นใจว่าบริษัทที่ถูกจัดจ้างมีมาตรการในการรักษาความปลอดภัยทุกขั้นตอนก่อนถูกทำลาย เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ที่ไม่ได้รับอนุญาต สำหรับเอกสารในรูปแบบ Soft file หรือการจัดเก็บข้อมูลในระบบของธนาคาร ในทางปฏิบัติอาจเป็นเรื่องยากที่จะทำการลบหรือทำลายข้อมูลให้หายไปและไม่สามารถกู้คืนได้อีก เอกสารฉบับนี้จึงจะเน้นถึงการทำข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ ซึ่งการกระทำดังกล่าวเป็นวิธีการที่ทำให้ข้อมูลส่วนบุคคลไม่ใช่ข้อมูลส่วนบุคคลอีกต่อไป เป็นหนึ่งในการบริหารความเสี่ยงของธนาคาร มีเทคนิคหลากหลายวิธี ดังที่จะกล่าวรายละเอียดในหัวข้อถัดไป

8.1 แนวปฏิบัติเกี่ยวกับการทำข้อมูลนิรนาม (Data Anonymization)

โดยทั่วไปแล้วการจัดทำข้อมูลนิรนาม หมายถึง กระบวนการในการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ คำศัพท์ที่ใช้ในแต่ละแหล่งอ้างอิงอาจแตกต่างกันไป ตัวอย่างเช่น บ้างใช้คำว่า การทำข้อมูลนิรนาม (Anonymization) และการขจัดตัวตน (De-Identification) สลับกัน บ้างก็ใช้คำว่า de-identification ว่าเป็นการอธิบายกระบวนการในการทำให้ข้อมูลไม่สามารถระบุตัวตนได้ และใช้คำว่า anonymization เพื่อแสดงถึงความจำเพาะของประเภทการ De-Identification ที่จะทำให้ไม่สามารถนำกลับมาระบุตัวบุคคลได้อีกครั้ง ไม่ว่าจะเป็นข้อมูลที่เป็นข้อมูลเดียวหรือข้อมูลที่ต้องนำไปรวมกับข้อมูลอื่นที่มีอยู่อีก

สำหรับวัตถุประสงค์หลักของแนวปฏิบัติฉบับนี้ คำว่า "Anonymization" หมายถึงกระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้ ทั้งนี้ข้อมูลที่ถูกทำการนิรนามทางกฎหมายจะไม่ถือเป็นข้อมูลส่วนบุคคลอีก ในกรณีที่ข้อมูลจะสามารถย้อนกลับมาเพื่อระบุ

ตัวตนได้หรือย้อนกลับไม่ได้ การทำให้ข้อมูลกลับมาระบุตัวตนของบุคคลได้นั้นเป็นสิ่งที่องค์กรต้องพิจารณาในการจัดการกับความเสี่ยงของข้อมูลที่สามารถกลับมาระบุตัวตนได้

เหตุผลในการทำข้อมูลให้อยู่ในรูปของข้อมูลนิรนาม (Anonymized Data) เพื่อให้ข้อมูลมีความเหมาะสมสำหรับการใช้งานมากกว่าสถานะเดิมของข้อมูลที่ถูกคุ้มครองภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น ข้อมูลที่ไม่สามารถระบุตัวตนได้ อาจถูกใช้เพื่อการทำวิจัยและการวิเคราะห์ข้อมูลจำนวนมาก ซึ่งการกระทำดังกล่าวไม่มีความจำเป็นที่จะต้องใช้ข้อมูลเพื่อการระบุตัวตน ดังนั้นชุดข้อมูลของ Anonymized Data ถือเป็นมาตรการในการบริหารความเสี่ยง ลดผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดความปลอดภัยของข้อมูล

ตัวอย่าง มาตรการเชิงเทคนิคในการรักษาความและปลอดภัยของข้อมูล

i. การแฝงข้อมูล (Pseudonymisation) คือการแทนที่สิ่งที่ระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลด้วยการอ้างอิงอื่น ๆ ตัวอย่างเช่น การแทนที่ชื่อบุคคล ด้วย รหัสหรือหมายเลขอ้างอิงที่สร้างขึ้นแบบสุ่ม ซึ่งข้อมูลทั้งสองชุดจะต้องถูกลดความสามารถในการเชื่อมโยงกัน ซึ่งเป็นหนึ่งในมาตรการในการรักษาความปลอดภัยของข้อมูล เพื่อลดความเสี่ยงและผลกระทบจากเหตุการณ์ถูกละเมิดข้อมูล ในความหมายของ GDPR หมายถึง กระบวนการประมวลผลข้อมูลในลักษณะที่ข้อมูลไม่สามารถระบุตัวบุคคลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ข้อมูลเพิ่มเติมอีกชุดควรทำการเก็บรักษาไว้แยกออกจากกัน ไม่ให้เข้าถึงข้อมูลได้ทั้งสองชุดเพื่อลดความสามารถในการเชื่อมโยงข้อมูลดังกล่าวในการกลับไประบุตัวเจ้าของข้อมูลส่วนบุคคลได้
ii. การรวมกลุ่มข้อมูล (Aggregation) แสดงค่าเป็นผลรวม ดังนั้นจึงไม่มีการแสดงค่าแต่ละค่าที่สามารถระบุตัวบุคคลได้ ตัวอย่างเช่นกำหนดชุดข้อมูลที่มีอายุแปดคน (เช่น 33, 35, 34, 37, 42, 45, 37, 40) แสดงผลรวมของอายุแต่ละบุคคลของจำนวนบุคคลทั้งหมดในกลุ่ม (เช่น 303) มากกว่าอายุของแต่ละบุคคลที่เป็นตัวแทนในชุดข้อมูลนี้
iii. การแทนที่ (Replacement) เป็นการแทนที่ค่าหรือเซตย่อยของค่าด้วยค่าเฉลี่ยที่คำนวณ ตัวอย่างเช่นแทนที่บุคคลด้วยอายุ 15, 18 และ 20 ด้วยค่าอายุ 17 เพื่อลดความแตกต่างของข้อมูลหากในกรณีที่อายุที่แท้จริงไม่ได้เป็นวัตถุประสงค์ในการใช้ข้อมูล
iv. การสกัดกั้นข้อมูล (Data Suppression) คือลบค่าที่ไม่จำเป็นสำหรับวัตถุประสงค์ในการใช้ข้อมูล ตัวอย่างเช่นการลบฟิลด์ "เชื้อชาติ" ออกจากชุดของข้อมูลส่วนบุคคล
v. การกล่าวอย่างกว้าง (Data recoding or generalization) คือการจัดกลุ่มหมวดหมู่เป็นหมวดหมู่ที่กว้างขึ้น การกล่าวเป็นช่วงของข้อมูล ตัวอย่างเช่นการจัดกลุ่มของระดับการศึกษาที่แน่นอน (เช่น ชั้นประถมศึกษา3 ชั้นมัธยมศึกษา2) ออกเป็นหมวดหมู่ที่กว้างขึ้น (เช่น ระดับ ประถมศึกษา มัธยมศึกษา ระดับปริญญาตรี) หรือซ่อนค่าภายในช่วงที่กำหนด (เช่นแทนที่อายุ 43 ' ด้วยช่วง '40 - 50 ')

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

vi. การสับเปลี่ยนข้อมูล (Data Shuffling) คือการผสมหรือแทนที่ค่ากับชนิดเดียวกันเพื่อให้ข้อมูลมีลักษณะคล้ายกัน แต่ไม่เกี่ยวข้องกับรายละเอียดที่แท้จริง ตัวอย่างเช่น นามสกุลในฐานข้อมูลลูกค้าสามารถถูกทำให้ไม่สามารถระบุตัวตนได้ โดยการแทนที่ด้วยนามสกุลที่มาจากฐานข้อมูลอื่น

vii. การบังข้อมูล (Masking) คือลบรายละเอียดบางอย่างในขณะที่รักษารูปลักษณ์ของข้อมูล ตัวอย่างเช่นการแสดงข้อมูลตัวเลขพาสปอร์ตเป็น '#####567A' แทนที่จะแสดง 'S1234567A' หรือการ บังข้อมูลหมายเลขโทรศัพท์เป็น '081xxxx678 แทนที่จะแสดง '0812345678'

อย่างไรก็ตาม กฎหมายมิได้กำหนดให้ใช้วิธีการใดวิธีการหนึ่งโดยเฉพาะหรือรับรองการใช้เทคนิคใด ๆ องค์กรจึงควรประเมินสถานการณ์และลักษณะการดำเนินธุรกิจเองและนำเทคนิคการรักษาความมั่นคงและปลอดภัยที่เหมาะสมที่มาใช้กับการดำเนินธุรกิจ

9. แนวปฏิบัติเกี่ยวกับข้อมูลที่มีการเก็บอยู่ก่อนแล้ว

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 95 กำหนดให้ "ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย"

สำหรับแนวปฏิบัติของข้อมูลที่มีอยู่ก่อนแล้ว ให้ธนาคารสามารถประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์เดิมที่เคยแจ้งต่อลูกค้าหรือตามความคาดหมายเดิมของลูกค้า ตัวอย่างเช่น เดิมธนาคารเคยส่งข้อมูลทางการตลาดให้กับลูกค้า เมื่อพระราชบัญญัติฉบับนี้มีผลบังคับใช้อย่างสมบูรณ์ ธนาคารยังสามารถส่งข้อมูลทางการตลาดให้กับลูกค้าได้ดังเดิม แต่จะต้องแจ้งถึงวิธีการยกเลิกความยินยอมให้ลูกค้าทราบ เพื่อให้ลูกค้าสามารถใช้สิทธิในการถอนความยินยอมได้ และหากลูกค้าถอนความยินยอมแล้วธนาคารจะประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ถูกถอนไปแล้วมิได้ เว้นแต่จะเข้าข้อยกเว้นตามกฎหมาย

10. แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

หากธนาคารได้รับการติดต่อจากเจ้าของข้อมูลส่วนบุคคล ในการร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ธนาคารอาจจัดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานรับเรื่องร้องเรียน หรือ Contact Center ของธนาคารทำหน้าที่ในการรับเรื่องร้องขอก็ได้

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดให้สิทธิของเจ้าของข้อมูลส่วนบุคคล มีดังต่อไปนี้ซึ่งสอดคล้องกับหลักการของ GDPR

- สิทธิในการถอนความยินยอม ("Right to Withdraw of Consent")
- สิทธิในการเข้าถึงข้อมูลส่วนบุคคล ("Right to Access")

- สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)
- สิทธิในการลบข้อมูลส่วนบุคคล (“Right to Erasure” or “Right to be Forgotten”)
- สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)
- สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)
- สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)
- สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (“Right to Restriction of Automated Individual Decision-Making, Including Profiling”) **

** สำหรับสิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียวนั้น ไม่ได้ถูกกล่าวถึงใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ดังนั้นสิทธิดังกล่าวไม่ได้อยู่ขอบเขตการบังคับใช้ของกฎหมายไทย

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิตามกฎหมายในการร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามที่ร้องขอ ซึ่งในรายละเอียดของการดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคลจะกล่าวถึงในรายละเอียดดังต่อไปนี้

10.1 สิทธิในการถอนความยินยอม (“Right to Withdraw of Consent”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอเพิกถอนความยินยอมที่จะให้ไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเมื่อใดก็ได้ และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการหยุดการประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคลเคยได้ให้ความยินยอมไว้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่มีฐานโดยชอบด้วยกฎหมายอื่น ที่จะทำการเก็บรวบรวม ใช้หรือเปิดเผยต่อไป ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบข้อมูลออก

การใช้สิทธิถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลควรดำเนินการโดยไม่ล่าช้านับแต่ที่ได้ทราบถึงการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยระยะเวลาในการปฏิตามสิทธิให้เป็นไปตามนโยบายที่เหมาะสมของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิกระทำได้ง่ายในระดับเดียวกับการให้ความยินยอม

10.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (“Right to Access”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มา ซึ่งข้อมูลดังกล่าวที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม เพื่อเป็นการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่า ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมไว้นั้นกำลังถูกประมวลผลหรือไม่อย่างไร เมื่อได้รับคำร้องขอแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตามคำร้องขอ โดยไม่ชักช้าภายใน 30 วัน นับแต่วันที่ได้รับการร้องขอ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาจกำหนดหลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนาหรือขยายระยะเวลาในการดำเนินการตามคำร้องขอตามความเหมาะสมได้ อย่างไรก็ตาม เพื่อเป็นแนวทางในการปฏิบัติในการดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลนี้ เอกสารฉบับนี้จึงอ้างอิงหลักเกณฑ์ตาม GDPR เกี่ยวกับสิทธิในการเข้าถึงและการขอรับสำเนาของข้อมูลส่วนบุคคลที่เกี่ยวกับตน ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีรายละเอียดดังต่อไปนี้

- วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ซึ่งบุคคลมีสิทธิที่จะทราบถึงฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลของตน
- ประเภทของข้อมูลส่วนบุคคล
- ประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผย โดยเฉพาะผู้รับข้อมูลในต่างประเทศหรือองค์การระหว่างประเทศ
- ระยะเวลาที่ในจัดเก็บข้อมูลส่วนบุคคล หรือ เกณฑ์ในการกำหนดระยะเวลาในการจัดเก็บข้อมูล
- การมีอยู่ของสิทธิของเจ้าของข้อมูลส่วนบุคคล อันได้แก่ สิทธิในการแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง สิทธิในการลบข้อมูล สิทธิในการห้ามมิให้ประมวลผล สิทธิในการคัดค้านการประมวลผลข้อมูล และสิทธิในการยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแล
- แหล่งที่มาของข้อมูลส่วนบุคคลกรณีได้รับมาจากแหล่งอื่น
- รายละเอียดที่เกี่ยวข้องกับการตัดสินใจอัตโนมัติและโปรไฟล์ลิ่ง (profiling) รวมถึงตรรกะเหตุผลที่ใช้ และผลที่คาดว่าจะเกิดขึ้นจากการประมวลผลด้วยวิธีการดังกล่าว

ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลมีสิทธิที่จะปฏิเสธคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีต่อไปนี้ และให้บันทึกการปฏิเสธคำร้องขอพร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 11.2.11

1. เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล
2. หากการใช้สิทธิในการเข้าถึงและการขอรับสำเนาข้อมูลส่วนบุคคลนั้น จะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น หากข้อมูลที่เก็บรวบรวมมีข้อมูลส่วนบุคคลของบุคคลที่สามรวมเกี่ยวข้องอยู่ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะไม่เปิดเผยข้อมูลเฉพาะของบุคคลที่สามได้ แต่ไม่สามารถปฏิเสธการเข้าถึงข้อมูลและขอรับสำเนาของเจ้าของข้อมูลส่วนบุคคลได้

ในการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลไม่ควรเรียกเก็บค่าธรรมเนียมใด ๆ ในการใช้สิทธิ เว้นแต่เจ้าของข้อมูลบุคคลมีการขอรับสำเนาเพิ่มเติม

มากจนเกินความจำเป็น ธนาคารอาจพิจารณาเรียกเก็บค่าธรรมเนียมในการจัดการได้ตามสมควรแก่กรณี

การใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ธนาคารควรพิจารณาให้มีช่องทางการร้องขอใช้สิทธิที่สาขาหรืออิเล็กทรอนิกส์ได้ตามสมควรแก่กรณี และการดำเนินการตามสิทธินั้นควรพิจารณาการให้ข้อมูลทางสาขาหรือทางอิเล็กทรอนิกส์ได้ตามสมควรด้วยเช่นกัน เพื่อให้ง่ายต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

10.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (“Right to Rectification”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลของตนที่ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด อันได้แก่

i. กรณีที่ข้อมูลไม่สมบูรณ์ คือการที่ข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่นั้นถูกต้องแต่ได้รับข้อมูลมาไม่ครบถ้วน ไม่เพียงพอต่อการนำไปประมวลผลตามวัตถุประสงค์
ii. กรณีที่ข้อมูลไม่ถูกต้อง คือการที่ข้อมูลไม่ตรงกับความจริง

ทั้งสองกรณี ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแก้ไขโดยไม่ชักช้า ในระหว่างการดำเนินการแก้ไขนั้น เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลชั่วคราวในระหว่างการตรวจสอบความถูกต้องของข้อมูล และดำเนินการแก้ไขข้อมูลส่วนบุคคลก่อนประมวลผลอีกครั้ง อย่างไรก็ตามเพื่อป้องกันผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลที่ไม่ถูกต้องผู้ควบคุมข้อมูลส่วนบุคคลควรระงับการประมวลผลแม้ว่าเจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ตาม นอกจากนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการแจ้งแก่บุคคลที่สามที่ข้อมูลส่วนบุคคลถูกเปิดเผย เช่น ผู้ประมวลผลข้อมูลส่วนบุคคลของธนาคาร ให้ทราบถึงการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลข้อมูลจะพิสูจน์ได้ว่าเป็นไปไม่ได้หรือเกินความพยายามตามสมควร

ทั้งนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 11.2.11

ในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง ธนาคารอาจกำหนดหลักเกณฑ์ในการพิสูจน์ความถูกต้องของข้อมูลส่วนบุคคล เช่น ให้เจ้าของข้อมูลส่วนบุคคลนำหลักฐานที่เกี่ยวข้องมาประกอบการพิจารณา อย่างไรก็ตาม แม้เจ้าของข้อมูลส่วนบุคคลจะมีสิทธิในการแก้ไข แต่ธนาคารยังคงมีหน้าที่ ที่ต้องดำเนินการตามหลักการในการประมวลผลข้อมูลส่วนบุคคลอย่างถูกต้อง Principle 4 : (“Accuracy”) เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ไม่ก่อให้เกิดความเข้าใจผิด และข้อมูลที่ไม่ถูกต้องจะต้องถูกลบหรือได้รับการแก้ไข ธนาคาร

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ควรตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลในขณะเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อลดความเสี่ยงและผลกระทบที่อาจทำให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลและกับธนาคารเอง

10.4 สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล (“Right to Erasure” or “Right to be Forgotten”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตน ธนาคารจะต้องดำเนินการดังกล่าว หากมีเหตุดังต่อไปนี้

- ข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคล ทำการถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและธนาคารไม่มีอำนาจตามกฎหมายที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยอีกต่อไป
- เจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ในกรณีที่เป็นข้อมูลส่วนบุคคลที่ธนาคารเก็บรวบรวม ไว้โดยได้รับยกเว้นไม่ต้องขอความยินยอมภายใต้ฐานภารกิจของรัฐ หรือ ฐานประโยชน์อันชอบธรรม และธนาคารไม่สามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ประโยชน์ สิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง
- เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย

หากเกิดเหตุข้างต้น ธนาคารจะต้องทำการลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้อีกโดยไม่ล่าช้า หากธนาคารได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยแก่สาธารณะ และธนาคารได้รับคำร้องขอใช้สิทธิดังกล่าว ธนาคารจะต้องรับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำร้องขอ โดยจะต้องทำการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ ทราบถึงการใช้สิทธิในการลบของเจ้าของข้อมูลส่วนบุคคล เพื่อดำเนินการลบหรือทำลายหรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

อย่างไรก็ตามธนาคารสามารถปฏิเสธคำร้องขอการใช้สิทธิในการลบหรือทำลายได้ หากพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นมีความจำเป็นในเรื่องดังต่อไปนี้

- ธนาคารพิสูจน์ได้ว่า การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลนั้นได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล
- เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ธนาคาร
- เป็นการจำเป็นเพื่อบรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์หรือประโยชน์ด้านสาธารณสุข

10.5 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (“Right to Restriction of Processing”)

เจ้าของข้อมูลส่วนบุคคล มีสิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคลของตน เมื่อเข้าเงื่อนไขดังต่อไปนี้

- เมื่อธนาคารอยู่ในระหว่างการตรวจสอบข้อมูล ตามคำร้องขอใช้สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- เมื่อเป็นข้อมูลที่ต้องทำการลบหรือทำลาย เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย แต่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการขอให้ระงับการใช้แทนการลบหรือทำลายข้อมูลส่วนบุคคลของตน
- เมื่อข้อมูลส่วนบุคคลไม่จำเป็นในการเก็บรักษาไว้ ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลอีกต่อไป แต่เจ้าของข้อมูลมีความจำเป็นที่ต้องขอให้การเก็บรักษาไว้ เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เมื่อธนาคารอยู่ในระหว่างการพิสูจน์ข้ออ้างที่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลนั้นมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล
- ธนาคารอยู่ในระหว่างการตรวจสอบเพื่อดำเนินการปฏิเสธการคัดค้านการประมวลผลของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่ธนาคารเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

บุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ว่าเป็นไปข้อยกเว้นที่ธนาคารสามารถประมวลผลได้เนื่องจากเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของธนาคาร

หากธนาคารปฏิเสธไม่ดำเนินการตามคำร้องขอใช้สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิได้

ธนาคารควรจัดให้มีมาตรการที่เหมาะสม ในการระงับการประมวลผลข้อมูลในระบบของธนาคาร เช่น การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว หรือการแยกส่วนข้อมูลที่ถูกระงับออกจากข้อมูลอื่นชั่วคราว เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกดำเนินการตามคำร้องขอ

10.6 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (“Right to Object”)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้านการประมวลผลข้อมูลของตนเมื่อใดก็ได้ เมื่อเข้าเงื่อนไขดังต่อไปนี้

1. เมื่อเป็นกรณีที่ข้อมูลส่วนบุคคลที่ธนาคารทำการเก็บรวบรวมได้รับยกเว้นไม่ต้องขอความยินยอม เฉพาะในกรณีดังนี้
   I. เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ธนาคาร
   II. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของธนาคารหรือของบุคคลอื่น

   <u>สามารถปฏิเสธคำร้องขอได้หาก</u> ธนาคารสามารถพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าผลประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล หรือการประมวลข้อมูลส่วนบุคคลนั้นทำเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

2. เป็นกรณีที่ ธนาคารทำการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการตลาดแบบตรง (Direct marketing) ในกรณีนี้ธนาคารจะ*<u>ไม่สามารถปฏิเสธคำร้องขอ</u>*ในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้
3. กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

   <u>สามารถปฏิเสธคำร้องขอได้หาก</u> เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของธนาคาร

หากธนาคารอ้างเหตุแห่งการปฏิเสธการคัดค้านการประมวลผลดังที่กล่าวมา ธนาคารจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 11.2.11

ในกรณีที่เจ้าของข้อมูลส่วนบุคคล ใช้สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล และธนาคารสามารถอ้างเหตุแห่งการปฏิเสธ ธนาคารจะไม่สามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปได้ และธนาคารจะต้องดำเนินการตามคำร้องขอ ซึ่งจะต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ทราบ

10.7 สิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคล (“Right to Data Portability”)

ลูกค้ามีสิทธิขอรับข้อมูลที่เกี่ยวกับลูกค้าจากธนาคาร ในกรณีที่ธนาคารได้ทำให้ข้อมูลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือ ใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรือ อุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ รวมทั้ง

10.7.1 มีสิทธิขอให้ธนาคารส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
<u>สามารถปฏิเสธคำร้องขอได้หาก</u> การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมาย หรือการใช้สิทธินั้นเป็นการละเมิดสิทธิเสรีภาพของบุคคลอื่น และธนาคารจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 11.2.11

10.7.2 ขอรับข้อมูลที่ธนาคารส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่สภาพทางเทคนิคไม่สามารถทำได้

ดังนั้น เพื่อประโยชน์ของทั้งเจ้าของข้อมูลส่วนบุคคลและประโยชน์แก่ธนาคารเอง ธนาคารจึงควรมีนโยบายและกระบวนการจัดการที่ชัดเจนในกรณีที่เจ้าของข้อมูลส่วนบุคคลมาขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ยกตัวอย่างเช่น ธนาคารอาจมอบหมายงานหรือจัดตั้งหน่วยงานภายใน ในการดูแล รับเรื่องร้องขอดังกล่าว แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เป็นผู้รับผิดชอบและพิจารณาการใช้สิทธิว่าสามารถดำเนินการให้ได้หรือไม่ และจัดให้มีช่องทางที่เหมาะสมในการยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

11. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Guideline on Data Controller and Data Processor Roles and Responsibilities)

11.1 การระบุสถานะในการคุ้มครองข้อมูลส่วนบุคคลของธนาคาร

ธนาคารอาจทำหน้าที่เป็นทั้งผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งขึ้นอยู่กับแต่ละกรณี อย่างไรก็ตามธนาคารจะต้องสามารถระบุสถานะให้ได้ว่า สำหรับชุดข้อมูลใดธนาคารเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล โดยสามารถพิจารณาจากการที่ธนาคารเป็นผู้ที่กำหนดวัตถุประสงค์และสามารถตัดสินใจในเรื่องของการประมวลผลข้อมูลส่วนบุคคลได้เองหรือไม่ หรือธนาคารทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลอื่น เนื่องจากการระบุสถานะเป็นสิ่งสำคัญพื้นฐานในการกำหนดหน้าที่ต่อไป โดยธนาคารสามารถพิจารณาได้ตามรายละเอียดใน Checklist ด้านล่างดังต่อไปนี้

<u>รายการตรวจสอบว่าธนาคารเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ (Data Controller Checklist)</u>

❒ ธนาคารเป็นผู้ตัดสินใจในเรื่องของการเก็บรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลได้

❒ ธนาคารสามารถกำหนดวัตถุประสงค์หรือผลลัพธ์จากการประมวลผลข้อมูลส่วนบุคคลที่ควรจะเป็นได้

❒ ธนาคารเป็นผู้ตัดสินใจได้ว่าควรเก็บรวบรวมข้อมูลส่วนบุคคลใดบ้าง

❒ ธนาคารเป็นผู้ตัดสินใจได้ว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลของใครบ้าง

❒ ธนาคารเป็นผู้ที่ได้รับประโยชน์เชิงเศรษฐกิจหรือประโยชน์อื่นจากการประมวลผลข้อมูล

❒ ธนาคารกระทำการประมวลผลข้อมูลภายใต้ข้อตกลงหรือสัญญาที่ได้ทำไว้กับเจ้าของข้อมูลส่วนบุคคล

❒ ธนาคารทำการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานธนาคาร

❒ ธนาคารเป็นผู้พิจารณาเกี่ยวกับผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคลจากการประมวลผลข้อมูลส่วนบุคคลของธนาคาร

❒ ธนาคารใช้ดุลยพินิจอย่างมืออาชีพในการประมวลผลข้อมูลส่วนบุคคล

❒ ธนาคารเป็นผู้ที่มีความสัมพันธ์เชิงธุรกิจโดยตรงกับเจ้าของข้อมูลส่วนบุคคล

❒ ธนาคารมีอิสระในการตัดสินใจเกี่ยวกับวิธีการประมวลผลข้อมูลส่วนบุคคล

❒ ธนาคารทำการแต่งตั้งผู้ประมวลผลข้อมูลเพื่อทำการประมวลผลข้อมูลส่วนบุคคลในนามของธนาคาร

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

<u>รายการตรวจสอบว่าธนาคารเป็นผู้ประมวลผลข้อมูลส่วนบุคคลหรือไม่ (Data Processor Checklist)</u>

❒ ธนาคารเป็นผู้ประมวลผลข้อมูลส่วนบุคคลตามคำแนะนำเกี่ยวกับการประมวลผลจากบุคคลอื่นหรือไม่

❒ ธนาคารได้รับข้อมูลส่วนบุคคลจากบุคคลที่สามหรือโดยผู้ที่กำหนดว่าธนาคารจะเก็บรวบรวมข้อมูลใดบ้าง

❒ ธนาคารไม่ได้เป็นผู้ตัดสินใจได้ว่าควรเก็บรวบรวมข้อมูลส่วนบุคคลใดบ้าง

❒ ธนาคารไม่ได้เป็นผู้ตัดสินใจได้ว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลของใครบ้าง

❒ ธนาคารไม่ได้เป็นผู้ที่กำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

❒ ธนาคารไม่ได้เป็นผู้กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

❒ ธนาคารไม่ได้เป็นผู้ตัดสินใจว่าข้อมูลส่วนบุคคลจะถูกเปิดเผยให้แก่ใคร

❒ ธนาคารไม่ได้เป็นผู้กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

❒ ธนาคารอาจทำการตัดสินใจในเรื่องของการประมวลผลข้อมูลอย่างไรแต่เป็นการทำภายใต้ข้อตกลงในสัญญาที่ได้ทำกับผู้อื่น

❒ ธนาคารไม่มีหน้าที่ทำการประเมินผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลที่อาจเกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล

11.2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller Roles and Responsibilities)

11.2.1 เมื่อธนาคารเป็นผู้ควบคุมข้อมูลส่วนบุคคล ธนาคารจะทำการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์อันชอบด้วยกฎหมาย นอกจากนั้นธนาคาร จะต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ทั้งมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ หรือเปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ และจะต้องมีการทบทวนมาตรการในการรักษาความปลอดภัยของข้อมูลเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงและปลอดภัยอย่างเหมาะสมอยู่เสมอ

11.2.2 ในกรณีที่ธนาคารต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ธนาคารจะต้องดำเนินการป้องกัน ไม่ให้ผู้นั้นนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยมิชอบ

11.2.3 ธนาคารจะต้องจัดให้มีระบบในการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาหรือที่ไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่จะทำการเก็บรักษาไว้ภายใต้ข้อยกเว้นตามกฎหมาย

11.2.4 หากเกิดเหตุการณ์ละเมิดขึ้น ธนาคารจะต้องแจ้งแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคล โดยไม่ชักช้าภายใน 72 ชั่วโมง นับจากที่ได้รับทราบเหตุ เว้นแต่การละเมิดนั้นไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล หากเหตุการณ์ละเมิดนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้ธนาคารรีบแจ้งเหตุละเมิดนั้นแก่เจ้าของข้อมูลส่วนบุคคลทราบด้วย รวมถึงแนวทางในการเยียวยาโดยเร็วที่สุด

11.2.5 ธนาคารต้องทำการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หากมีการประมวลผลข้อมูลส่วนบุคคล มีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักของธนาคารเป็นการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว นอกจากนั้นธนาคารจะต้องให้ข้อมูลการติดต่อ DPO ไว้ใน Privacy Notice/ Privacy Policy ของธนาคารด้วย เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อ DPO ได้ หากมีความประสงค์จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่าง ข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ในส่วนของ Privacy Notice/ Privacy Policy “หากมีข้อสงสัยเกี่ยวกับข้อมูลส่วนบุคคลหรือมีความประสงค์ที่จะใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเราได้ตามรายละเอียดการติดต่อด้านล่างนี้ *เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)* : นาย ข. *อีเมล*: dataprotectionofficer@ABCbank.com *โทร*: 1234”

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ธนาคารสามารถดูรายละเอียดเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ในหัวข้อ "12. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)"

11.2.6 ธนาคารจะต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ในกรณีที่การประมวลผลข้อมูลมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ธนาคารจะต้องมีการจัดทำ DPIA สามารถดูรายละเอียดเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลได้ในหัวข้อ "13. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)"

11.2.7 ธนาคารมีหน้าที่ในการดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลมีการร้องขอใช้สิทธิ ในการรับเรื่องร้องขอจากเจ้าของข้อมูลส่วนบุคคล ธนาคารอาจกำหนดให้มีผู้ที่รับผิดชอบในเรื่องดังกล่าวอย่างชัดเจน เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หน่วยงานรับเรื่องร้องเรียน หน่วยงานลูกค้าสัมพันธ์ เป็นต้น เพื่อจัดให้มีการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า หากธนาคารปฏิเสธคำร้องขอตามเหตุแห่งการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลนั้น ธนาคารจะต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล พร้อมด้วยเหตุผลตามที่ระบุในหัวข้อ 11.2.11

11.2.8 ธนาคารจะต้องทำการเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัยของข้อมูล

11.2.9 ธนาคารจะต้องจัดให้มีการทำข้อตกลงกันระหว่างธนาคาร (ผู้ควบคุมข้อมูลส่วนบุคคล) และผู้ประมวลผลข้อมูลส่วนบุคคล หรือที่เรียกว่า Data Processing Agreement เพื่อให้ผู้ประมวลผลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย

11.2.10 หากธนาคารมีการโอนข้อมูลไปยังต่างประเทศหรือธนาคารระหว่างประเทศจะต้องทำโดยชอบด้วยกฎหมาย นั่นคือจะต้องมั่นใจว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ สามารถดูรายละเอียดเพิ่มเติมได้ในหัวข้อ "6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Cross-Border Data Transfer)"

11.2.11 ธนาคารจะต้องทำการจัดให้มีการเก็บบันทึกข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการบันทึกข้อมูลที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ตามหลักการ

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ ธนาคารจะต้องทำการบันทึกรายการอย่างน้อยดังต่อไปนี้

1. ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล
6. การใช้หรือเปิดเผย
7. การปฏิเสธคำขอหรือการคัดค้านตามข้อกำหนดของกฎหมาย
8. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

สำหรับหน้าที่ในการเก็บบันทึกได้รับยกเว้นให้กับกิจการขนาดเล็ก โดยอ้างอิงจาก GDPR ที่ว่าหากธนาคารมีจำนวนลูกจ้างน้อยกว่า 250 คน ให้ถือเป็นกิจการขนาดเล็ก อย่างไรก็ตามหากการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือมีการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หรือเป็นการประมวลผลข้อมูลอาชญากรรม ให้ธนาคารทำการเก็บบันทึกการประมวลผลข้อมูลส่วนบุคคล

11.2.12 หากธนาคารอยู่นอกราชอาณาจักร แต่อยู่ภายใต้บังคับของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จะต้องแต่งตั้งตัวแทนของธนาคารต่างประเทศ (ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล) เป็นหนังสือซึ่งตัวแทนจะต้องอยู่ในราชอาณาจักรและจะต้องได้รับมอบอำนาจให้กระทำการแทนธนาคารที่อยู่นอกราชอาณาจักรโดยไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของธนาคารที่อยู่นอกราชอาณาจักร จะได้รับยกเว้นไม่ต้องแต่งตั้งตัวแทนในราชอาณาจักรในกรณีที่ธนาคารที่อยู่นอกราชอาณาจักรไม่ได้มีการประมวลผลข้อมูลที่เกี่ยวข้องกับข้อมูลอ่อนไหว และไม่ได้ประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

11.2.13 ธนาคารมีหน้าที่ในการให้ความร่วมมือกับองค์กรกำกับดูแล หรือทำหน้าที่ตามกฎหมายตามคำสั่งของหน่วยงานรัฐหรืออำนาจโดยชอบในการเข้าถึงข้อมูล

11.2.14 กรณีธนาคารได้มีการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกอื่นใด แต่ละฝ่ายจะมีหน้าที่และความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากกันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

11.3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Roles and Responsibilities)

ในกรณีที่ธนาคารทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล ในนามของผู้ควบคุมข้อมูลส่วนบุคคลอื่น ซึ่งธนาคารจะต้องทำการประมวลผลข้อมูลตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) หากธนาคารทำการประมวลผลนอกเหนือหรือขัดต่อคำสั่งของผู้ควบคุมข้อมูล การกระทำดังกล่าวให้ถือว่าธนาคารทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลนั้น ซึ่งธนาคารก็จะต้องปฏิบัติตามหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลสำหรับกรณีดังกล่าวด้วย

ในกรณีที่ธนาคารมีสถานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ธนาคารจะต้องปฏิบัติตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามแนวปฏิบัติดังต่อไปนี้

11.3.1 ธนาคารจะต้องดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น ไม่ทำการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากที่ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลหากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร เว้นแต่คำสั่งดังกล่าวนั้นขัดต่อกฎหมาย

11.3.2 ธนาคารจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสม มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การใช้ เปลี่ยนแปลง แก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

11.3.3 ธนาคารจะต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด เว้นแต่ธนาคารเป็นกิจการขนาดเล็ก โดยอ้างอิงจาก GDPR ที่ว่าหากกิจการมีจำนวนลูกจ้างน้อยกว่า 250 คน ให้ถือเป็นกิจการขนาดเล็ก อย่างไรก็ตามหากการประมวลผลข้อมูลนั้นอาจก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวหรือเป็นการประมวลผลข้อมูลอาชญากรรม ให้ธนาคารทำการเก็บบันทึกการประมวลผลข้อมูลส่วนบุคคล ธนาคารจะต้องจัดให้มีรายละเอียดการเก็บบันทึกรายการประมวลผลข้อมูลส่วนบุคคลจะต้องมีดังต่อไปนี้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

1. ชื่อและข้อมูลการติดต่อธนาคารและผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

2. ประเภทการประมวลผลซึ่งทำแทนผู้ควบคุมข้อมูลส่วนบุคคล
3. การส่งข้อมูลไปยังต่างประเทศ (หากมี)
4. คำอธิบายเกี่ยวกับมาตรการเชิงเทคนิคและเชิงบริหารจัดการเกี่ยวกับการรักษาความมั่นคงและปลอดภัยของข้อมูลส่วนบุคคล

11.3.4 ธนาคารต้องทำการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หากมีการประมวลผลข้อมูลส่วนบุคคล มีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักของธนาคารเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว

11.3.5 ธนาคารจะต้องทำการแจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลเกิดการรั่วไหล (Data Breach) ธนาคารจะต้องทำการแจ้งโดยไม่ชักช้าหลังจากทราบเหตุ และธนาคารไม่มีหน้าที่ต้องแจ้งแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล

12. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

ธนาคารจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อการคุ้มครองสิทธิประโยชน์ของธนาคารและเพื่อคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคล นอกจากนั้นการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะช่วยให้องค์กรสามารถบริหารความเสี่ยงและจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและประสิทธิผล

12.1 การแต่งตั้งและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ธนาคารสามารถที่จะจัดแต่งตั้งบุคคลหรือคณะทำงานจากบุคลากรของธนาคารเอง หรือจัดจ้างบุคคลภายนอกก็ได้ ซึ่งบุคคล/คณะทำงานดังกล่าวจะต้องมีความรู้ความเข้าใจในด้านกฎหมายการคุ้มครองข้อมูลส่วนบุคคล มีความเข้าใจกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของธนาคาร การรักษาความปลอดภัยของข้อมูลส่วนบุคคล งานด้านเทคโนโลยีสารสนเทศ อีกทั้งเข้าใจถึงภาพรวมธุรกิจของธนาคารและมีความสามารถในการสร้างวัฒนธรรมขององค์กรในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

หากธนาคารมีความประสงค์ที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันกับกลุ่มเครือกิจการ นั้นสามารถทำได้ โดยธนาคารหรือกลุ่มเครือกิจการจะต้องสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

12.2 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Responsibility of DPO)

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นมีหน้าที่ดังต่อไปนี้

1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล (ซึ่งหมายถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรให้คำแนะนำแก่พนักงานทุกคนของธนาคาร รวมถึงผู้รับจ้างให้ทำการประมวลผลข้อมูลส่วนบุคคลของธนาคาร) เกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
2) ทำการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
3) ประสานงานและให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

นอกจากนั้นเพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นไปได้อย่างมีประสิทธิภาพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรได้รับการสนับสนุนการปฏิบัติงานจากธนาคาร โดยการให้อำนาจหน้าที่ และมีความเป็นอิสระในการทำงาน มีสายการรายงานที่ตรงไปยังผู้บริหารสูงสุดของธนาคารได้ อีกทั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจมีความจำเป็นที่จะต้องได้รับสิทธิในเข้าถึงข้อมูลส่วนบุคคลที่จำเป็นเพื่อการปฏิบัติหน้าที่ ธนาคารจึงควรแสดงให้เห็นถึงความสำคัญของหน้าที่ดังกล่าว เพื่อให้พนักงานทุกคนตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และให้ความร่วมมือในการปฏิบัติหน้าที่กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยการให้ข้อมูลหรือแจ้งเหตุความเป็นไปได้ที่จะเกิดการละเมิดของข้อมูลส่วนบุคคล หรือปัญหาต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบและเพื่อหาแนวทางการแก้ไขต่อไป

13. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

การประมวลผลข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง ดังนั้นการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Protection Impact Assessment (DPIA) นั้นเป็นหนึ่งในกระบวนการที่ธนาคารต้องจัดให้มีสำหรับการประมวลผลที่มีความเสี่ยงสูง เพื่อเป็นการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งสอดคล้องกับ GDPR

การจัดทำ DPIA ที่มีประสิทธิภาพนั้นจะช่วยให้ธนาคารสามารถกำกับการปฏิบัติตามกฎเกณฑ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลส่วนบุคคลและส่วนรวมมากขึ้น ช่วยลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม ลดความเสี่ยงที่จะเกิดผลกระทบต่อชื่อเสียงของธนาคาร ซึ่งจะเป็นผลดีแก่ธนาคารเอง

13.1 ความแตกต่างระหว่าง Data Protection Impact Assessment (DPIA) กับ Privacy Impact Assessment (PIA)

- **Data Protection Impact Assessment (DPIA)** เป็นกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล สำหรับกิจกรรมประมวลผลข้อมูลส่วนบุคคลต่าง ๆ ซึ่งตามกฎหมายกำหนดให้ทำเฉพาะกับความเสี่ยงสูง นั่นก็คือมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งธนาคารสามารถขอคำปรึกษาจาก DPO ในขั้นตอนการออกแบบและการจัดทำ DPIA กระบวนการในจัดทำ DPIA ได้แก่ การระบุความเสี่ยงและผลกระทบที่อาจเกิดขึ้น (สำหรับการระบุความเสี่ยงและประเมินผลกระทบที่อาจเกิดขึ้น โปรดดูรายละเอียดในหัวข้อ 3.2 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล) รวมถึงแนวทางการลดความเสี่ยงที่อาจเกิดขึ้นจากกิจกรรมการประมวลผลนั้น การทำ DPIA ไม่ใช่กระบวนการที่ทำเพียงครั้งเดียวแต่จะต้องมีการทบทวนความเหมาะสมอยู่เสมอ เนื่องจากความเสี่ยงอาจเปลี่ยนแปลงได้จากปัจจัยหลายอย่าง เช่น การเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็วอาจทำให้ความเสี่ยงที่จะเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลสูงขึ้น เป็นต้น
- **Privacy Impact Assessment (PIA)** เป็นกระบวนการที่เกี่ยวข้องกับการวิเคราะห์ การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลว่าจะทำอย่างไร โดยที่ PIA เป็นกระบวนการที่ใช้ในการป้องกันในเรื่องของการจัดทำ Privacy by Design นั่นก็คือ การที่ธนาคารจะต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบ ซึ่งมักทำเมื่อมีการเริ่มหรือเข้าควบรวมกิจการอื่น มีการใช้กระบวนการใหม่ หรือออกผลิตภัณฑ์ใหม่

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

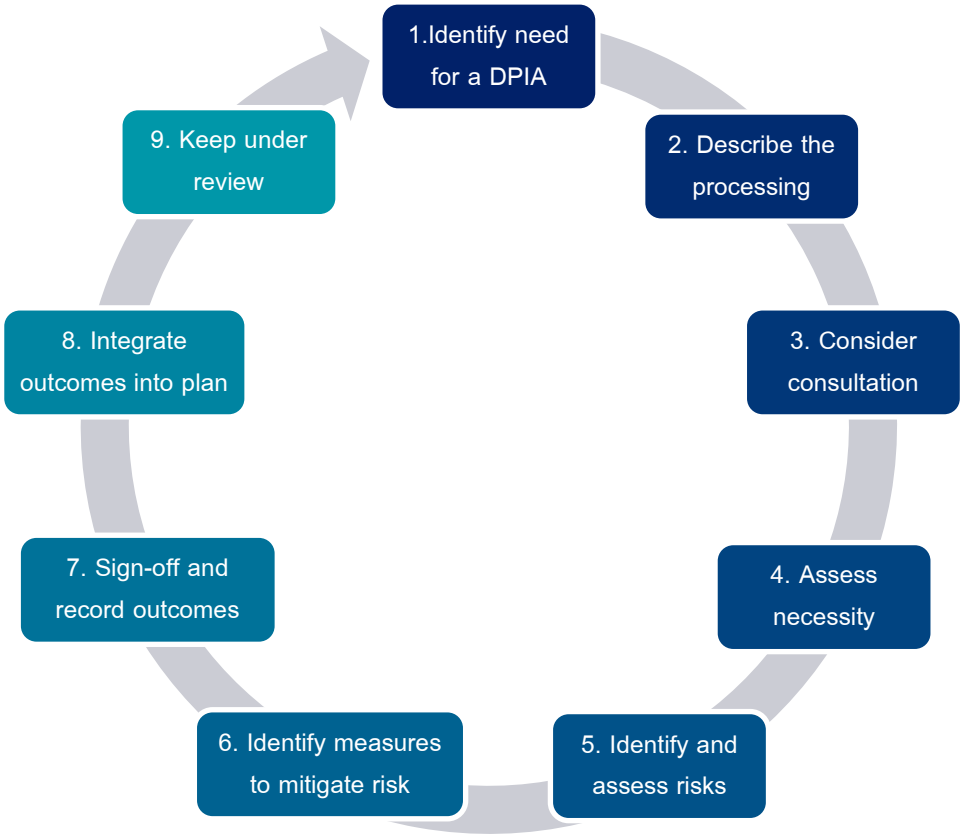
ธนาคารอาจทำ DPIA เพียงอย่างเดียวก็ได้หรืออาจจัดทำ PIA เข้ากับ DPIA ก็ได้เนื่องจากแนวทางในการจัดทำนั้นมีความคล้ายคลึงกัน อย่างไรก็ตาม ธนาคารอาจพิจารณาการทำ PIA เพิ่มเติมเมื่อเห็นว่ามีความจำเป็น

13.2 แนวปฏิบัติเกี่ยวกับการจัดทำ DPIA

แนวปฏิบัติฉบับนี้ได้ อ้างอิงหลักการจาก GDPR ในการจัดทำ DPIA ซึ่งกำหนดให้กระบวนการจัดทำจะต้องปฏิบัติตาม 4 ขั้นตอนต่อไปนี้เป็นอย่างน้อย

1. ธนาคารจะต้องทำการระบุรายละเอียดของกิจกรรมการประมวลผลอย่างเป็นระบบ อันได้แก่ กระบวนการหรือวิธีการประมวลผลข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูล และประโยชน์อันชอบด้วยกฎหมายของธนาคาร
2. การประเมินความจำเป็นและสัดส่วนในการใช้ข้อมูลอย่างเหมาะสม ที่เกี่ยวข้องกับการประมวลผลตามวัตถุประสงค์
3. การประเมินความเสี่ยงที่อาจเกิดผลกระทบกับความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
4. แนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น รวมถึงมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจว่าธนาคารมีการคุ้มครองสิทธิเสรีภาพและประโยชน์อันของธรรมของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ หากธนาคารพิจารณาแล้วว่าระดับของความเสี่ยงนั้นสูงเกินกว่าที่ธนาคารสามารถจัดให้มีมาตรการในการลดความเสี่ยงนั้นได้ ธนาคารควรพิจารณาไม่กระทำการประมวลผลข้อมูลส่วนบุคคลหรือปรึกษาคณะกรรมคุ้มครองข้อมูลส่วนบุคคลก่อน

การจัดทำ DPIA เป็นกระบวนการที่ธนาคารควรเริ่มจัดทำก่อนการทำการประมวลผลข้อมูล และดำเนินการควบคู่ไปกับกระบวนการวางแผนและพัฒนา และทำอย่างต่อเนื่อง หากขั้นตอนในการจัดทำ DPIA มีความละเอียดและชัดเจน ก็จะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการประมวลผลข้อมูลอย่างเหมาะสม ธนาคารอาจพิจารณาขั้นตอนในการจัดทำ DPIA เพิ่มเติมตามดังภาพด้านล่าง เพื่อใช้ในการจัดทำ DPIA ได้อย่างครอบคลุมยิ่งขึ้น



ขั้นตอนในการจัดทำ DPIA (Steps carry out a DPIA)

ในการพิจารณาการจัดทำ DPIA นั้นได้กำหนดให้จำเป็นต้องทำเมื่อมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ซึ่งธนาคารสามารถพิจารณากิจกรรมการประมวลผลที่เข้าข่ายเป็นกิจกรรมที่มีความเสี่ยงสูงได้ ตามหลักการของ GDPR ดังต่อไปนี้

- Systematic and Extensive Profiling with Significant Effects
  การประมวลผลข้อมูลด้วยระบบอัตโนมัติ หรือ การทำ Profiling ที่อาจมีผลกระทบอย่างมีนัยสำคัญ
- Process Special Category or Criminal Offence Data on a Large Scale
  การประมวลผลข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลประวัติอาชญากรรม ข้อมูลพฤติกรรมทางเพศ เป็นจำนวนมาก
- Systematically Monitor Publicly Accessible Places on a Large Scale
  ระบบการตรวจตราที่ใช้เฝ้าดูพื้นที่สาธารณะเป็นจำนวนมาก เช่น ศูนย์การค้า ห้องสมุด

กรอบในการพิจารณาที่จะช่วยในการตัดสินใจของธนาคารว่าในกรณีใดธนาคารมีความจำเป็นที่ต้องทำ DPIA สามารถทำตามมาตรฐานสากลของ GDPR กำหนดให้หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเข้าข่ายตามเกณฑ์ที่ระบุตั้งแต่ 2 ข้อขึ้นไป

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

1. (Evaluation or Scoring) เป็นกระบวนการทำโปรไฟลิ่งหรือการประเมินผลหรือให้คะแนนโดยระบบอัตโนมัติ และการใช้ข้อมูลส่วนบุคคลเพื่อการคาดการณ์ (prediction) โดยเฉพาะเมื่อการประมวลผลนั้นมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเชิงลึก เช่น พฤติกรรม, ความชอบ, สุขภาพ, หรือ ตำแหน่งที่ตั้ง เป็นต้น
2. (Automated-Decision Making with Legal or Similar Significant Effect) หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการใช้เทคโนโลยีเพื่อทำการตัดสินใจอัตโนมัติ ในเรื่องที่ส่งผลกระทบกับกฎหมายหรือในเรื่องที่ส่งผลกระทบกับบุคคลอย่างมีนัยสำคัญ เช่น อาจทำให้ถูกเลือกปฏิบัติ
3. (Systematic Monitoring) ระบบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ การติดตาม การสังเกต สอดส่อง หรือควบคุมบุคคล โดยเฉพาะในพื้นที่ที่บุคคลสาธารณะสามารถเข้าถึงได้ (Public Accessible Area) เช่น ระบบเฝ้าระวังหรือตรวจตราในพื้นที่สาธารณะ โดยที่บุคคลไม่อาจทราบถึงหรือไม่รู้ล่วงหน้าว่ามีกิจกรรมการประมวลผลนี้ หรือไม่ทราบว่ามีผู้ควบคุมข้อมูลส่วนบุคคลเป็นใครและกำลังทำอะไรอยู่ ส่งผลให้เป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะสามารถหลีกเลี่ยง หรือ ปฏิเสธการมีส่วนร่วมได้
4. (Sensitive Data) เมื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับข้อมูลอ่อนไหว เช่น เชื้อชาติ, เผ่าพันธุ์, ประวัติอาชญากรรม, ความเห็นทางการเมือง เป็นต้น (โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ 5.4 ข้อมูลอ่อนไหว) เนื่องจากการประมวลผลข้อมูลดังกล่าว
5. (Data Processed on a Large Scale) หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก โดยพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง, ปริมาณข้อมูลหรือเนื้อหาของข้อมูลส่วนบุคคล, ระยะเวลาของกิจกรรมประมวลผล, และ ขอบเขตทางภูมิศาสตร์ของกิจกรรมการประมวลผล
6. (Datasets That Have Been Matched or Combined) ชุดข้อมูลที่เกิดจากการรวบรวมหรือเปรียบเทียบข้อมูลส่วนบุคคลที่มาจากแหล่งข้อมูลหลายแหล่ง ที่มีวัตถุประสงค์ในการประมวลผลข้อมูลต่างกัน ข้อมูลที่ถูกนำมารวมหรือเปรียบเทียบไม่จำกัดว่าเป็นข้อมูลที่ถูกประมวลผลแล้ว และไม่จำกัดว่าแหล่งข้อมูลมาจากธนาคารเองแต่อาจมาจากผู้ควบคุมข้อมูลอื่นก็ได้ ซึ่งการทำเช่นนี้อาจทำให้การประมวลผลข้อมูลส่วนบุคคลนั้นผิดจากวัตถุประสงค์ที่ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลไว้ในตอนแรก อีกทั้งอาจไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคลได้
7. (Data Concerning Vulnerable Data Subjects) หากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับผู้เปราะบาง (Vulnerable Person) เช่น ผู้เยาว์ ผู้อพยพ ผู้ป่วยทางจิต หรือผู้สูงวัย GDPR ให้จัดว่ากิจกรรมการประมวลผลนั้นมีความเสี่ยงที่จะทำให้เกิดผลกระทบต่อ

เจ้าของข้อมูลส่วนบุคคล เนื่องจากผู้เปราะบางอาจไม่อยู่ในสภาพที่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลได้ รวมถึงการทำโปรไฟลิ่งข้อมูลของผู้เยาว์หรือการให้บริการออนไลน์แก่ผู้เยาว์โดยเฉพาะเพื่อวัตถุประสงค์การทำการตลาดแบบตรง

8. (Innovative Use or Applying Technological or Organizational Solutions) เมื่อมีการประมวลผลข้อมูลส่วนบุคคลซึ่งเกิดจากเทคโนโลยีใหม่ที่มีการใช้อย่างกว้างขวางในชีวิตประจำวันของเจ้าของข้อมูลส่วนบุคคล เช่น การ สแกนลายนิ้วมือ และใบหน้า ซึ่งอาจจะนำไปสู่ความเสี่ยงที่นอกเหนือความคาดหมายได้ เนื่องด้วยเทคโนโลยีดังกล่าวยังไม่เคยปรากฏหรือใช้มาก่อน ธนาคารจึงอาจไม่มีข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นได้ต่อเจ้าของข้อมูลส่วนบุคคล
9. (Data Transfer Across Borders) หากมีการโอนข้อมูลไปยังต่างประเทศ สามารถดูรายละเอียดเพิ่มเติมได้ที่หัวข้อ “6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ” นอกจากธนาคารจะต้องพิจารณากฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางแล้ว ยังต้องพิจารณาถึงความเป็นไปได้ที่ข้อมูลนั้นอาจถูกส่งต่อด้วย
10. (Prevents Data Subjects from Exercising a Right or Using a Service or a Contract) หากกิจกรรมการประมวลผลนั้นอาจส่งผลให้เกิดการเปลี่ยนแปลงหรืออาจถูกปฏิเสธสิทธิของเจ้าของข้อมูล หรืออาจถูกปฏิเสธการได้รับบริการหรือการเข้าทำสัญญาของเจ้าของข้อมูล เช่น ธนาคารมีกระบวนการคัดกรองลูกค้า จากการประมวลผลข้อมูลของลูกค้ากับฐานข้อมูลของธนาคาร เพื่อตรวจสอบข้อมูลเครดิตและตัดสินใจว่าจะให้ลูกค้าเข้าทำสัญญาเงินกู้กับธนาคารหรือไม่

อย่างไรก็ตามในกรณีที่กิจกรรมประมวลผลข้อมูลนั้นเข้าข่ายตามเกณฑ์ที่ได้ระบุไว้มากกว่าสองข้อ ธนาคารสามารถเลือกที่จะไม่ทำ DPIA ได้ หากพิจารณาแล้วว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะไม่ส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล โดยธนาคารควรที่จะทำการปรึกษากับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนเพื่อพิจารณาถึงความเหมาะสม รวมถึงทำการจดบันทึกถึงเหตุผลที่ธนาคารใช้ในการตัดสินใจไม่ทำ DPIA หรือกรณีที่แม้เข้าข่ายเพียงหนึ่งข้อแต่อาจส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงกับเจ้าของข้อมูลส่วนบุคคล ธนาคารก็จำเป็นจะต้องจัดทำ DPIA

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตัวอย่าง แบบฟอร์มการทำ DPIA

1. จุดประสงค์ในการจัดทำ DPIA

อธิบายอย่างละเอียดถึงกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง วัตถุประสงค์ และประเภทของการประมวลผลข้อมูล และระบุเหตุผลที่ในการจัดทำ DPIA สำหรับกิจกรรมการประมวลผลนั้น และหากมีเอกสารที่เกี่ยวข้องโปรดแนบมาพร้อมแบบฟอร์มนี้ :

……
……
……

2. รายละเอียดของกิจกรรมการประมวลผล

(Nature of data processing) ระบุรูปแบบของกิจกรรมการประมวลผลที่เกี่ยวข้อง โดยอธิบายถึงรายละเอียดหากคุณจะมีการเก็บรวบรวม ใช้ เปิดเผย หรือ ทำลายข้อมูลส่วนบุคคล และโปรดระบุหากมีการส่งต่อข้อมูลส่วนบุคคลไปยังองค์กรอื่น และส่วนไหนของกิจกรรมการประมวลผลข้อมูล นั้นพิจารณาแล้วว่ามีความเสี่ยงสูง

……
……
……

(Scope) ขอบเขตของกิจกรรมการประมวลผลข้อมูล อธิบายถึงรูปแบบในการประมวลผลข้อมูลส่วนบุคคลที่มีความเกี่ยวข้อง โดยระบุหากข้อมูลส่วนบุคคลนั้นนับว่าเป็นข้อมูลอ่อนไหว เช่น ประวัติอาชญากรรมหรือ ข้อมูลทางด้านสุขภาพ และโปรดระบุถึงรายละเอียดการเก็บรวบรวมหรือใช้ของข้อมูลที่เกี่ยวข้องในแง่ของปริมาณ ความถี่ในการเก็บรวบรวม ระยะเวลาในการจัดเก็บ และมีเจ้าของข้อมูลส่วนบุคคลกี่คนที่อาจจะได้รับผลกระทบ

……
……
……

(Context) ระบุถึงบริบทของกิจกรรมการประมวลผล โดยอธิบายถึงความสัมพันธ์ระหว่างองค์กรและเจ้าของข้อมูลส่วนบุคคล ขอบเขตของการควบคุมที่เจ้าของข้อมูลส่วนบุคคลมีความคาดหมายของเจ้าของข้อมูลส่วนบุคคลต่อกิจกรรมการประมวลผลนี้ เจ้าของข้อมูลส่วนบุคคลนั้นมีกลุ่มของเยาวชนหรือบุคคลอ่อนไหวหรือไม่ และโปรดระบุหากมีเคยมีการแจ้งองค์กรถึงความเสี่ยงต่อกิจกรรมการประมวลผลนี้

……
……
……

(Purpose) อธิบายถึงจุดประสงค์ของกิจกรรมการประมวลผลข้อมูลนี้ จุดมุ่งหมายของคุณคืออะไร, ผลกระทบที่น่าจะเกิดต่อเจ้าของข้อมูลส่วนบุคคล, และ ผลประโยชน์ที่องค์กรจะได้รับจากกิจกรรมการประมวลผลนี้

.....

.....

.....

3. การพิจารณาความจำเป็นและสัดส่วนของกิจกรรมการประมวลผลที่เหมาะสม

(Nature) ระบุถึงมาตรการ และ ฐานกฎหมายที่ใช้ในกิจกรรมการประมวลผล โดยอธิบายถึงความเกี่ยวข้องระหว่างกิจกรรมการประมวลผลและเป้าหมายของกิจกรรมการประมวลนั้น และโปรดระบุหากมีวิธีการอื่นที่จะช่วยให้องค์กรบรรลุจุดมุ่งหมายดังกล่าวได้นอกเหนือจากกิจกรรมการประมวลผลนั้น คุณมีมาตรการอย่างไรในการแจ้งและการสนับสนุนการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

.....

.....

.....

4. การพิจารณาและประเมินความเสี่ยง

อธิบายถึงที่มาของความเสี่ยงและผลกระทบที่น่าจะเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล

.....

.....

.....

<u>ความน่าจะเป็นที่ผลกระทบจะเกิดขึ้น (Likelihood)</u>

❒ โอกาสต่ำ ❒ โอกาสปานกลาง ❒ โอกาสสูง

<u>ความร้ายแรงของผลกระทบ (Severity)</u>

❒ ไม่ร้ายแรง ❒ ร้ายแรงปานกลาง ❒ ร้ายแรงมาก

<u>ความเสี่ยงโดยรวม (Overall Risk)</u>

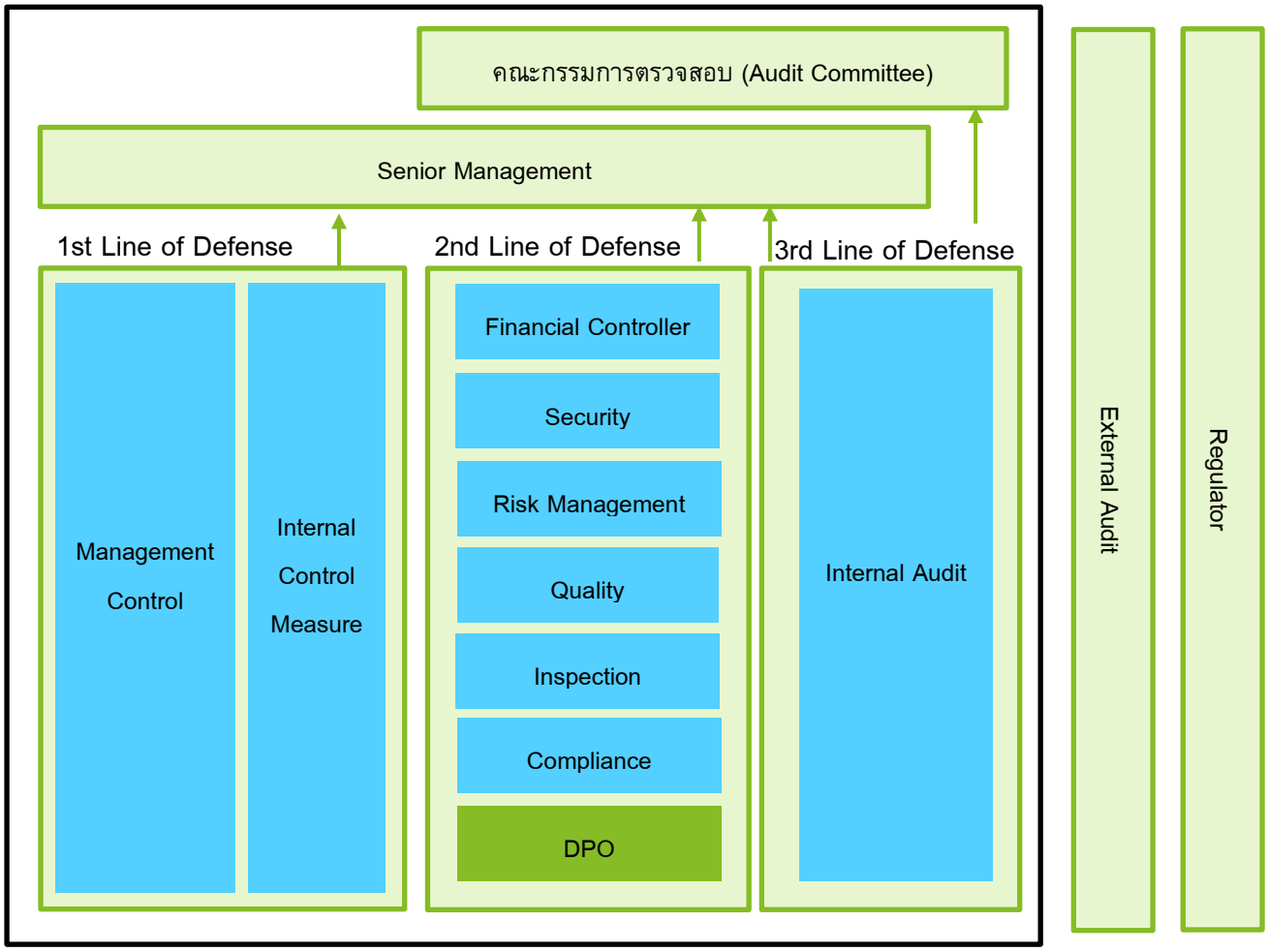
ความเสี่ยงต่ำ	ความเสี่ยงสูง	ความเสี่ยงสูง
ความเสี่ยงต่ำ	ความเสี่ยงปานกลาง	ความเสี่ยงสูง
ความเสี่ยงต่ำ	ความเสี่ยงต่ำ	ความเสี่ยงต่ำ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

14. แนวปฏิบัติเกี่ยวกับ Three Lines of Defense สำหรับการบริหารจัดการข้อมูลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

เพื่อให้การบริหารจัดการข้อมูลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นผลสำเร็จ ธนาคารจะต้องจัดให้มีการแบ่งหน้าที่ในเรื่องของการป้องกันและการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างชัดเจน เพื่อให้แน่ใจว่าพนักงานทุกคนทราบและตระหนักถึงหน้าที่และความรับผิดชอบของตนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างเหมาะสม

แนวปฏิบัติฉบับนี้ ได้นำหลักการจาก Federation of European Risk Management Associations (FERMA) มาใช้เป็นแนวทางในการกำหนดแนวปฏิบัติเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ซึ่งกำหนดให้ DPO จะต้องปฏิบัติหน้าที่อย่างเป็นกลาง มีความเป็นอิสระจากการประมวลผลข้อมูลส่วนบุคคล ไม่ทำหน้าที่ในการกำหนดวัตถุประสงค์รวมทั้งวิธีในการประมวลผลข้อมูล



Three Lines of Defense Model

จากรูปแบบการแบ่งแนวป้องกัน Three Lines of Defense Model กำหนดให้

- หน่วยงานปฏิบัติงาน (Operational Function) ทำหน้าที่ในการกำหนดวัตถุประสงค์และวิธีการในการดำเนินการในการประมวลผลข้อมูลส่วนบุคคล ทำหน้าที่เป็นแนวป้องกันแรก (First Line of Defense)
- หน่วยงานบริหารความเสี่ยงความเสี่ยง (Risk Management Function) ทำหน้าที่เป็นแนวป้องกันที่สอง (Second Line of Defense)
- หน่วยงานตรวจสอบภายใน (Internal Audit Function) ทำหน้าที่เป็นแนวป้องกันที่สาม (Third Line of Defense)
- กำหนดให้ DPO Function ทำหน้าที่เป็นแนวป้องกันที่สอง

First Line of Defense: สำหรับ First Line of Defense เป็นหน้าที่ของสายงานธุรกิจ เช่น หน่วยงานปฏิบัติงาน เพื่อทำหน้าที่ในการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล และทำหน้าที่ในการบันทึกข้อมูลลงในระบบฐานข้อมูลของธนาคาร และเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล อีกทั้งรับผิดชอบในการตรวจสอบคุณภาพของข้อมูลที่เก็บรวบรวม เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องครบถ้วน ตามข้อกำหนดของกฎหมาย และเป็นไปตามข้อกำหนดของหน่วยงานกำกับดูแลข้อมูลของธนาคาร

Second Line of Defense: สำหรับ Second Line of Defense ทำหน้าที่ในการควบคุมกำกับดูแลธนาคารในภาพรวม เช่น ทำหน้าที่กำกับดูแลการปฏิบัติงาน วางแนวทาง กรอบแนวคิด เงื่อนไขและขั้นตอนปฏิบัติงานให้กับ First Line of Defense คอยสอดส่อง ตรวจตราหาช่องว่างในการปฏิบัติงาน ที่ส่วนที่ไม่ชัดเจน (Gray Areas) ของธนาคารเพื่อหาทางป้องกันและแก้ไข รวมทั้งเพื่อกำหนดแนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น หน่วยงานที่ทำหน้าที่เป็น Second Line of Defense ได้แก่ หน่วยงานกำกับ หน่วยงานบัญชีและการเงิน หน่วยงานด้าน IT หน่วยงานบริหารบุคคล หน่วยงานวางแผนงบประมาณ หน่วยงานงานบริหารอาคารสถานที่ หน่วยงานบริหารความเสี่ยง รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

กำหนดให้หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นหน้าที่ที่อยู่ใน Second Line of Defense ซึ่งธนาคารอาจแต่งตั้งเป็นบุคคลหรือหน่วยงานก็ได้ เช่น สำนักงานข้อมูลส่วนกลาง (Central Data Office) หน่วยงานกำกับดูแลข้อมูล (Data Governance Function) สำนักงานจัดการข้อมูล (Data Management Office) หรือ ผู้ดูแลข้อมูลระดับสูง (Chief Data Officer) เป็นต้น ซึ่งหน้าที่ของบุคคลหรือหน่วยงานคุ้มครองข้อมูลส่วนบุคคล จะทำหน้าที่ในการควบคุม กำกับ การประมวลผลข้อมูล เช่น กำหนดนโยบายที่เกี่ยวข้องกับการบริหารจัดการข้อมูล บริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และกำหนดตัวชี้วัดคุณภาพของข้อมูล รวมทั้งทำการติดตามผล เพื่อเป็นการสร้างกลไกในการยกระดับ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

มาตรฐานในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล และเพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย และเป็นไปตามนโยบายของธนาคารเอง นอกจากนี้ ยังทำหน้าที่เป็นผู้ที่ให้คำปรึกษาในเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเมื่อมีความจำเป็น เช่น เมื่อจะมีการออกแบบวิธีการประมวลข้อมูลแบบใหม่ เมื่อต้องมีการประเมินผลกระทบที่อาจเกิดขึ้นต่อเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจากการเปลี่ยนแปลงของเทคโนโลยีและรูปแบบการดำเนินธุรกิจ เป็นต้น รวมถึงหน้าที่ในการติดต่อประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สามารถดูรายละเอียดเพิ่มเติมเกี่ยวกับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ในหัวข้อ “12.2 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Responsibility of DPO)”

Third Line of Defense: สำหรับ Third Line of Defense ธนาคารสามารถจัดให้เป็นบุคคลหรือหน่วยงาน เพื่อทำหน้าที่ในการตรวจสอบภายใน เพื่อให้มั่นใจว่าธนาคารมีการปฏิบัติงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการบริหารความเสี่ยง เป็นไปตามข้อกำหนดของกฎหมายและนโยบายที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของธนาคาร และเพื่อให้มั่นใจว่าธนาคารมีนโยบายที่เพียงพอและเหมาะสม สำหรับโครงสร้างของสายการรายงานสำหรับหน่วยงานที่ทำหน้าที่ในการตรวจสอบ ธนาคารควรกำหนดให้หน่วยงานดังกล่าวสามารถรายงานตรงต่อคณะกรรมการตรวจสอบได้ ในกรณีที่เกิดเหตุการณ์ที่อาจกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ธนาคารอาจกำหนดให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานอื่นใด ในการรายงานต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลตามแต่ธนาคารจะเห็นสมควร

15. เหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)

การรั่วไหลของข้อมูลส่วนบุคคล หมายถึง การที่ข้อมูลส่วนบุคคลถูกทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บ รักษาหรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

ในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลเกิดขึ้นภายในธนาคาร ผู้ที่ทราบเหตุจะต้องมีการแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการรั่วไหล รวมทั้งออกมาตรการเยียวยาเหตุการณ์รั่วไหลของข้อมูล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลส่วนบุคคลและ/หรือสำนักงานคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกการรั่วไหลของข้อมูลส่วนบุคคล และประเมินความเสี่ยงเมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคลขึ้น ในการประเมินความเสี่ยงจากการรั่วไหลของข้อมูลนั้น อาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล เนื่องจากหากพิจารณาแล้วว่า ไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องมีการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลหรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลที่เกิดขึ้น แต่หากผล

ของการประเมินแสดงให้เห็นว่าการรั่วไหลของข้อมูลอาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้งแก่เจ้าของข้อมูลส่วนบุคคลรวมทั้งแนวทางในการเยียวยาอีกทั้งแจ้งเหตุละเมิดของข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา 72 ชั่วโมง นับจากทราบเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

ธนาคารควรมีการจัดทำแบบฟอร์มบันทึกการรั่วไหลของข้อมูลส่วนบุคคล ขึ้นเพื่อเป็นแนวทางในการจดบันทึกอย่างถูกต้องและครบถ้วน สำหรับหน้าที่ในการจดบันทึกควรกำหนดให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือในกรณีที่พนักงานผู้พบเหตุการณ์รั่วไหลของข้อมูลอาจให้พนักงานผู้พบเหตุการณ์เป็นผู้ทำการบันทึกแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้แล้วแต่กรณี และแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การรั่วไหลของข้อมูลที่เกิดขึ้นด้วย เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการหาสาเหตุและมาตรการเยียวยา รวมถึงติดตามผลการดำเนินงานการแก้ไขปัญหาการรั่วไหลของข้อมูล

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ตัวอย่าง แบบฟอร์มการบันทึกการรั่วไหลของข้อมูลส่วนบุคคล

โปรดระบุรายละเอียดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

วันและเวลาที่คุณพบการรั่วไหล : .....

โปรดอธิบายอย่างละเอียดถึงเหตุการณ์ที่เกิดขึ้น :

.....

.....

คุณพบการรั่วไหลได้อย่างไร :

.....

วันและเวลาที่การรั่วไหลเกิดขึ้น : .....

ประเภทของเจ้าของข้อมูลส่วนบุคคล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

❒ ลูกค้า ❒ พนักงาน

❒ ผู้เยาว์ ❒ ไม่ทราบแน่ชัด

❒ อื่น ๆ (โปรดระบุ) .....

ประเภทของข้อมูลที่เกิดการรั่วไหล (เลือกทุกข้อที่มีความเกี่ยวข้อง)

❒ ข้อมูลทั่วไป เช่น ชื่อ ข้อมูลติดต่อ ❒ เอกสารทางการ เช่น บัตรประชาชน

❒ Usernames, Passwords ❒ ข้อมูลด้านการเงิน เช่น เลขบัตรเครดิต

❒ ข้อมูล GPS locations ❒ ข้อมูลเกี่ยวกับเชื้อชาติ หรือ สัญชาติ

❒ ข้อมูลด้านความคิดเห็นทางการเมือง ❒ ข้อมูลเกี่ยวกับศาสนา

❒ ข้อมูลเกี่ยวกับเพศ ❒ ข้อมูลเรื่องสุขภาพ

❒ ข้อมูลทางชีวภาพ ❒ ประวัติอาชญากรรม

❒ ยังไม่ทราบ ❒ อื่น ๆ (โปรดระบุ) .....

ปริมาณโดยสังเขปของข้อมูลที่รั่วไหล : .....

ปริมาณโดยสังเขปของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ :

.....

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่น่าจะเกิดจากการรั่วไหล :

.....

ความน่าจะเป็นที่การรั่วไหลของข้อมูลส่วนบุคคลจะส่งผลกระทบที่เป็นการคุกคามต่อเจ้าของข้อมูลส่วนบุคคล :

❒ เป็นไปได้สูง

❒ เป็นไปได้

❒ เป็นกลาง

❒ เป็นไปได้ต่ำ

❒ เป็นไปไม่ได้

❒ ไม่ทราบแน่ชัด

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่อาจจะเกิด หรือ เกิดไปแล้วต่อเจ้าของข้อมูลส่วนบุคคล

……

……..

หากมีการล่าช้าในการแจ้งเหตุการณ์การรั่วไหลเกิดขึ้นโปรดชี้แจงเหตุผล

……

……..

จงอธิบายมาตรการที่ได้บังคับใช้ในการควบคุมการรั่วไหลที่เกิดขึ้น

……

……..

ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลหรือไม่

❒ มีการแจ้งเจ้าของข้อมูลส่วนบุคคลเรียบร้อยแล้ว

❒ อยู่ในระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล

❒ มีการตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล

❒ อยู่ในระหว่างการตัดสินใจขององค์กร

❒ อื่น ๆ (โปรดระบุ) ……..

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

ได้มีการแจ้งคณะกรรมการหรือองค์กรที่เกี่ยวข้องถึงเหตุการณ์การรั่วไหลหรือไม่

❒ มีการแจ้ง

❒ ไม่มีการแจ้ง

❒ ยังไม่ทราบแน่ชัด

หากตอบว่ามีการแจ้ง โปรดชี้แจงรายละเอียด

……

……..

……..

16. คำถามที่พบบ่อย

คำถาม	คำตอบ
16.1 กรณีที่ธนาคารให้บริการลูกค้านิติบุคคล เช่น ปล่อยกู้ หรือทำ Syndicate Loan ธนาคารมีความจำเป็นต้องเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของบุคลากร (เช่น กรรมการ ตัวแทน พนักงานที่มีส่วนเกี่ยวข้องกับธุรกรรม ฯลฯ) ของลูกค้านิติบุคคลเพื่อให้ธุรกรรมของนิติบุคคลเสร็จสมบูรณ์และธนาคารไม่ได้เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่น ธนาคารสามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของบุคลากรของลูกค้านิติบุคคลดังกล่าวภายใต้ฐาน Contractual Basis และไม่ต้องปฏิบัติมาตรา 25 รวมทั้งไม่ต้องขอความยินยอมในการเปิดเผยข้อมูลเพื่อทำให้ธุรกรรมเสร็จสมบูรณ์	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.2 คำถาม กรณีที่ธนาคารให้บริการซื้อขายอัตราแลกเปลี่ยนให้แก่ลูกค้านิติบุคคล ธนาคารมีความจำเป็นต้องเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของบุคลากรของลูกค้าดังกล่าวเพื่อให้ธุรกรรมซื้อขายอัตราแลกเปลี่ยนเสร็จสมบูรณ์ (ธนาคารไม่ได้เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่น) ในบางกรณี ที่ลูกค้าต้องการซื้อขายผ่าน Trading Platform ธนาคารต้องเปิดเผยข้อมูลของบุคลากรเหล่านี้ไปนิติบุคคลต่างประเทศที่ไม่อยู่ในกลุ่มธุรกิจเดียวกับธนาคารเพื่อ Sign Up เข้าใช้ระบบซื้อขายอัตราแลกเปลี่ยนแทนลูกค้านิติบุคคล ธนาคารสามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของบุคลากรของลูกค้านิติบุคคลดังกล่าวภายใต้ฐาน Contractual Basis	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.3 คำถาม กรณีที่ธนาคารแนะนำให้ลูกค้านิติบุคคลให้แก่บริษัท A เพื่อให้ทำธุรกรรมที่นอกเหนือจากธุรกิจของธนาคาร (Referral Scheme) ซึ่งธนาคารต้องเก็บรวบรวม ใช้และเปิดเผยข้อมูลของบุคลากรของลูกค้าดังกล่าว ให้แก่บริษัท A เพื่อให้บริษัท A ติดต่อกับบุคลากรของลูกค้าของธนาคารประเด็นที่จะเสนอให้เพิ่มใน TBA PDPA Guideline: สามารถให้ธนาคารเก็บรวบรวม ใช้และเปิดเผยข้อมูลของบุคลากรของลูกค้านิติบุคคลดังกล่าวภายใต้ฐาน Legitimate Interest	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้การเปิดเผยข้อมูลบุคลากรของลูกค้านิติบุคคลได้ โดยธนาคารต้องมีการพิจารณา 3 past test ก่อนที่จะในหลักประโยชน์โดยชอบธรรม Legitimate Interest ปรับใช้ แต่ทั้งนี้ลูกค้านิติบุคคลจะต้องให้ความยินยอมแก่ธนาคารในการเปิดเผยข้อมูลตามเกณฑ์ Market Conduct ด้วย

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

16.4 คำถาม บริษัท Leasing ในเครือของธนาคารได้นำส่งข้อมูลลูกค้าของบริษัทดังกล่าวเพื่อให้ธนาคารประเมินความเสี่ยงต่อกลุ่มธุรกิจของธนาคาร ซึ่งธนาคารได้ใช้ข้อมูลของลูกค้า (ของบริษัทในเครือดังกล่าว) ที่มีอยู่กับธนาคารด้วย มาใช้เพื่อประเมินและบริหารความเสี่ยงได้แม่นยำขึ้น แล้วธนาคารจะนำส่งผลลัพธ์กลับไปให้แก่บริษัทในเครือเพื่อบริหารความเสี่ยงให้เหมาะสมต่อไป เช่น ธนาคารอาจจะนำส่งวงเงินของลูกค้าดังกล่าวให้แก่บริษัทในเครือเพื่อให้บริษัทในเครือปรับเพิ่ม/ลด exposure ที่มีต่อลูกค้าให้เหมาะสมต่อไป ธนาคารสามารถดำเนินการดังกล่าวได้โดยใช้ Legitimate Interest ได้หรือไม่	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.5 คำถาม ธนาคารทำการประมวลผลข้อมูลส่วนบุคคลเพื่อการป้องกัน รับมือ ลดความเสี่ยงที่อาจเกิดการกระทำผิดกฎหมายต่างๆ ซึ่งรวมถึงการแบ่งปันข้อมูลส่วนบุคคลเพื่อยกระดับมาตรฐานการทำงานของอุตสาหกรรมธนาคารพาณิชย์ ในการป้องกันรับมือความเสี่ยงข้างต้น เช่น การตรวจสอบการทุจริต (**Fraud Prevention)** ธนาคารอาจมีการเปิดเผยข้อมูลของบุคคลที่มีความเสี่ยงในการทุจริตหรือมีประวัติการทุจริตให้กับธนาคารพาณิชย์อื่นๆ ในอุตสาหกรรมธนาคารพาณิชย์ ภายใต้ข้อตกลงในการรักษาข้อมูลความลับ ธนาคารสามารถดำเนินการดังกล่าวได้โดยไม่ต้องขอความยินยอมได้หรือไม่	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.6 คำถาม ธนาคารจะทำการประเมินราคาทรัพย์สินที่ลูกค้าจะนำมาใช้เป็นหลักประกัน เพื่อนำผลประเมินราคา มาพิจารณาประกอบการให้สินเชื่อและเพื่อการจัดชั้นและการกันเงินสำรองของสถาบันการเงิน ในการประเมินราคาดังกล่าวธนาคารอาจมอบหมายให้บริษัทภายนอก ไปดำเนินการประเมินราคาแทนธนาคาร โดยบริษัทประเมินราคาภายนอกจะต้องมีคุณสมบัติตามหลักเกณฑ์ที่ ธปท.กำหนด ธนาคารสามารถดำเนินการดังกล่าวได้โดยใช้ Legitimate Interest ได้หรือไม่	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.7 คำถาม ธนาคารอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งสาธารณะ เพื่อดำเนินการเรื่อง AML ธนาคารสามารถดำเนินการดังกล่าวได้โดยไม่ต้องขอความยินยอม (ตามมาตรา 25) ได้หรือไม่	คำตอบ ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้

16.8 คำถาม เนื่องจากธนาคารต้องประเมินราคาที่ดินที่เป็นหลักประกัน โดยธนาคารต้องประเมินและรวบรวมที่ดินโดยรอบเพื่อความแม่นยำในการประเมินราคา อย่างไรก็ตาม การเก็บข้อมูลที่ดินโดยรอบนั้น ธนาคารมีความจำเป็นต้องเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องจากแหล่งต่างๆ เช่น การประกาศขายในสื่อสาธารณะ ตัวแทนและนายหน้าขายที่ดิน หรือบริษัทประเมินราคาที่ดิน ธนาคารสามารถดำเนินการดังกล่าวได้โดยไม่ต้องขอความยินยอม (ตามมาตรา 25) ได้หรือไม่	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.9 คำถาม คำถามนิยามลักษณะจากข้อความใน Guidline ""สามารถแสดงให้เห็นถึงความเหมาะสมในการใช้ข้อมูล และมีผลกระทบเพียงเล็กน้อยต่อความเป็นส่วนตัวของบุคคล และบุคคลสามารถคาดหมายต่อกิจกรรมเหล่านั้นของธนาคารได้ หรือบุคคลไม่มีแนวโน้มที่จะคัดค้านกิจกรรมการประมวลผลเหล่านั้นได้"" อย่างไรเพื่อให้ธนาคารสามารถใช้ฐานประโยชน์อันชอบธรรมเพื่อให้สามารถประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาดได้ การที่ธนาคารแจ้งลูกค้าว่าจะนำข้อมูลที่ลูกค้ากรอกในใบสมัครหรือบอกทางวาจาหรือให้กับธนาคารด้วยวิธีอื่นๆว่าจะนำข้อมูลไปประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาดได้ให้ลูกค้าทราบ และลูกค้าไม่ได้มีท่าทีคัดค้านใดๆ ถือว่าธนาคารสามารถใช้ประโยชน์อันชอบธรรมโดยไม่ต้องขอความยินยอม(consent) ได้ใช่หรือไม่	คำตอบ ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.10 การเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวก่อน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ธนาคารต้องทำอย่างไร	ข้อมูลอ่อนไหวที่ได้รับมาก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับท่านต้องพิจารณาว่าท่านสามารถอาศัยฐานใดในการจัดเก็บและใช้ข้อมูลเหล่านั้นต่อไป โดยหลักแล้ว ท่านสามารถดำเนินการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม อย่างไรก็ดี หากเป็นกรณีที่ข้อมูลดังกล่าวจะต้องอาศัยความยินยอมโดยชัดแจ้ง ท่านในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย ตามมาตรา 95

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

16.11 Transfer and Transit แตกต่างกันอย่างไร	*Transfer* กรณีเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศหรือองค์การระหว่าง ประเทศ ในทางทฤษฎีข้อมูลที่ถูกส่งหรือโอนผ่านทางอินเทอร์เน็ตไปยังต่างประเทศนั้นจะ เกิดขึ้นในลักษณะของการส่งหน่วยย่อยของข้อมูล (data packets) ไปยังประเทศปลายทางโดยผ่านเครือข่าย อินเทอร์เน็ต การส่งข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ตนั้นจะเริ่มต้นจาก การที่ข้อมูลในประเทศผู้ส่งนั้นถูกแปลงให้กลายเป็นหน่วยย่อย (packets) (ในลักษณะของการบรรจุสินค้าลงกล่องโดยระบุหมายเลขที่ใช้สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ (IPaddress) ของผู้ส่ง) เพื่อกระบวนการดังกล่าวเสร็จสิ้นหน่วยย่อยของข้อมูลดังกล่าวจะถูกส่งจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ของผู้รับโดยผ่านเครือข่ายต่าง ๆ ซึ่งจะแสดงผลโดยประกอบ (assemble) หน่วยย่อยของข้อมูลในรูปแบบที่ถูกจัดเรียงเอาไว้ก่อนหน้านี้ (pre-specified sequence) *Transit* การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในกรณีของการส่งอีเมลหรือวิธีการเข้าถึงทางไกลแบบอื่นนั้นจะเป็นกรณีที่ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในประเทศไทยนั้นถูกแปลงเป็นหน่วยย่อยและถูกส่งไปเพื่อแสดงผลบนอุปกรณ์ (เช่นเครื่องคอมพิวเตอร์) ของผู้รับข้อมูล จากลักษณะของการส่งหรือโอนข้อมูลข้างต้น การส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลที่อยู่ในประเทศไทยโดยทางอีเมลไปยังผู้รับโอนข้อมูลซึ่งอยู่ในประเทศไทยนั้นย่อมไม่มีลักษณะเป็นการส่งหรือโอนข้อมูลบุคคลไปยังต่างประเทศตามกฎหมาย แม้ว่าข้อมูลส่วนบุคคลจากเดินทางผ่านเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งตั้งอยู่ต่างประเทศ เนื่องจากไม่ได้ มีการแสดงผลหรือเข้าถึงข้อมูลส่วนบุคคลในประเทศที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ตั้งอยู่
16.12 Binding Corporate Rule มีหลักการอย่างไร	ในกรณีที่กฎหมาย องค์กร หรือพันธกรณีในระดับนานาชาติของประเทศปลายทางยังไม่มี ความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล (ผู้โอน) อาจทำ “นโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน”

	หากนโยบายดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลได้ "บุคคลผู้อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจ ร่วมกัน" นั้นอาจอ้างอิงเกณฑ์ "บริษัทในเครือ" ตามแนวทางของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ก็ได้ แต่สาระสำคัญของเรื่องนี้ก็คือเครือกิจการหรือเครือธุรกิจนั้นได้ทำความตกลงกันที่จะผูกพันตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ หรือที่เรียกว่า BCR (Binding Corporate Rules) หลักการพื้นฐานสำหรับการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ 1. มีสภาพบังคับตามกฎหมายและกำหนดหน้าที่ที่ชัดเจนของสมาชิกในกลุ่มที่จะต้องปฏิบัติ รวมถึงลูกจ้างและพนักงานของสมาชิก 2.รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลและการบังคับใช้สิทธิในฐานะผู้รับประโยชน์ ภายนอก รวมถึงการใช้สิทธิร้องเรียนต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลและศาล 3.เครือกิจการจะต้องแสดงว่าตนสามารถรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากสมาชิกของเครือกิจการ 4. เจ้าของข้อมูลส่วนบุคคลในฐานะผู้รับประโยชน์ภายนอกสามารถเข้าถึงข้อมูลทั้งหลายที่เกี่ยวกับการใช้สิทธิของตน 5. แสดงมาตรการอบรมและให้ความรู้แก่ลูกจ้างและพนักงานของกิจการ 6. มีมาตรการรับเรื่องร้องเรียนที่เหมาะสมเพียงพอ 7.มีการตรวจสอบและประเมินการปฏิบัติตาม BCR 8. กำหนดหน้าที่ในการให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล 9. อธิบายขอบเขตของการ BCR รวมถึง สภาพของการส่งหรือโอนข้อมูล, ประเภทเจ้าของข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต 10. มาตรการคุ้มครองข้อมูลส่วนบุคคล รวมถึงความรับผิดชอบ และความสัมพันธ์ เกี่ยวข้องกับกฎหมายภายในประเทศ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

16.13 กรณี1. ตัวแทนจำหน่ายรถยนต์ ส่งข้อมูลต่อไปนี้ให้ธนาคาร เพื่อพิจารณาผู้ซื้อรถที่ประสงค์จะขอสินเชื่อในเบื้องต้น (ยังไม่พิจารณาเครดิต) • ชื่อ - นามสกุล เลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ และรายละเอียดเกี่ยวกับรถยนต์พร้อมใบสั่งจองรถ ธนาคารจะแจ้งผลผ่านเจ้าหน้าที่ธนาคาร เพื่อแจ้งพนักงานขายของตัวแทนจำหน่ายดังกล่าวด้วยวาจา 2. ธนาคารจะแจ้งผลการพิจารณาสินเชื่อ (หลังพิจารณาเครดิต) โดยแจ้งข้อมูลชื่อ - นามสกุล และ/หรือเงื่อนไขการเช่าซื้อที่อนุมัติให้ตัวแทนจำหน่ายรถยนต์ทราบ (กรณีอนุมัติสินเชื่อ) เพื่อแจ้งลูกค้าและนัดมอบรถยนต์หรือหาผู้ให้สินเชื่อรายใหม่ต่อไป	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.14 การโทรไปยังนายจ้างของลูกค้าที่มาขอสินเชื่อหรือการโทรไปยังนายจ้างของผู้ที่มาสมัครงานกับสถาบันการเงิน เพื่อทำการยืนยันสถานภาพการเป็นพนักงานปัจจุบัน และในทางกลับกันกรณีสถาบันการเงินต้องตอบคำถามดังกล่าวให้แก่สถาบันการเงินที่ลูกค้าไปขอสินเชื่อหรือบริษัทที่พนักงานไปสมัครงาน สถาบันการเงินสามารถดำเนินการได้ภายใต้ฐานทางกฎหมายใดและภายในขอบเขตใดสามารถอ้างฐาน Legitimate Interest ได้หรือไม่	ประเด็นดังกล่าวข้างต้นสามารถนำหลักการประโยชน์โดยชอบธรรม Legitimate Interest มาปรับใช้ได้ โดยธนาคารต้องมีการพิจารณา 3 Part Test ก่อนที่จะนำหลักการประโยชน์โดยชอบธรรมมาปรับใช้
16.15 การดำเนินการเพื่อรองรองรับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	โปรดพิจารณาเอกสารแนบ Appendix B
16.16 การทำ Data Encryption and Anonymization	โปรดพิจารณาเอกสารแนบ Appendix C

ภาคผนวก ง. เอกสารอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ 2563
- Thailand Data Protection Guidelines 1.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กันยายน 2561 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- Thailand Data Protection Guidelines 2.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตุลาคม 2562 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ธันวาคม 2563 ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- กรอบในการประเมินระดับความพร้อมรับมือภัยคุกคามไซเบอร์สำหรับผู้ประกอบธุรกิจ (Cyber Resilience Assessment Framework- "CRAF") เวอร์ชัน 1.1 และคำอธิบาย โดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)
- กรอบการประเมินความพร้อมด้าน Cyber Resilience ภายใต้หลักเกณฑ์การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Management) ของสถาบันการเงิน โดยธนาคารแห่งประเทศไทย (ธ.ป.ท.)
- Data Governance for Government ธรรมาภิบาลข้อมูลภาครัฐ เวอร์ชัน 1.0 โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
- The General Data Protection Regulation (Regulation (EU) 2016/679) (‘GDPR’)
- Data Protection Directive 95/46/EC of the European Parliament and of the Council (General Data Protection Regulation)
- Information Commissioner’s Office (ICO) Guidance available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- NIST Federal Information Processing Standards Publication (FIPS PUB 199) : Standards for Security Categorization of Federal Information and Information Systems available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

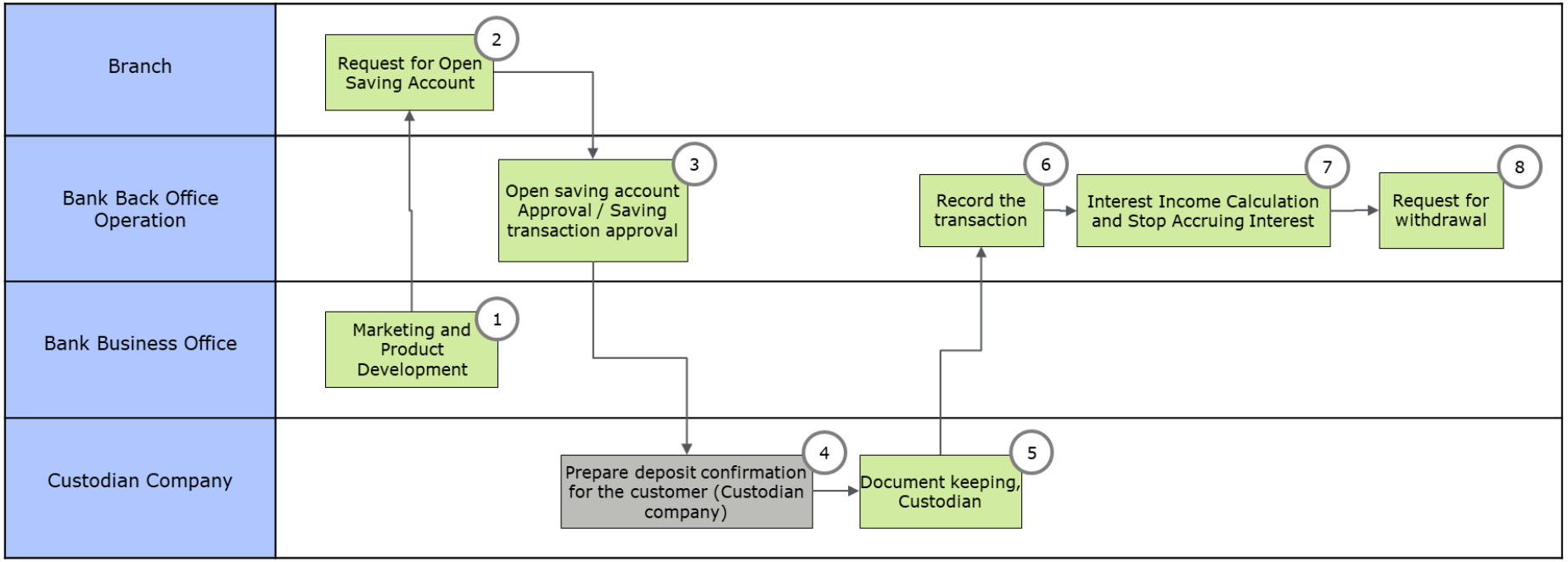
- NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- NISTIR 8053 De-Identification of Personal Information available at http://dx.doi.org/10.6028/NIST.IR.8053
- Malta Bankers' Association Data Protection Guidelines for Banks May 2018
- Malaysia Personal Data Protection Code Of Practice For The Banking And Financial Sector
- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- The Guide to the General Data Protection Regulation (GDPR) by Information Commissioner's Office (ICO)
- GDPR for marketers: Consent and Legitimate Interests Published by The Direct Marketing Association (UK) Ltd Copyright © Direct Marketing Association
- Hong Kong Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry by Office of the Privacy Commissioner for Personal Data
- Guidelines on Data Protection Officers ('DPOs') - ARTICLE 29 DATA PROTECTION WORKING PARTY 16/EN WP 243 rev.01
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 - ARTICLE 29 DATA PROTECTION WORKING PARTY 17/EN WP 248
- Guidelines on Personal data breach notification under Regulation 2016/679 - ARTICLE 29 DATA PROTECTION WORKING PARTY 18/EN WP250rev.01
- FERMA's Views on the Guidelines on Data Protection Officers Adopted on 13 December 2016 by the Article 29 Data Protection Working Party, 15 February 2017 by The Federation of European Risk Management Associations (FERMA)
- Guidelines on personal data breach notification For the European Union Institutions and Bodies by European Data Protection Supervisor (EDPS)

- Advisory Guideline on the Personal Data Protection Act for Selected Topics, Issued 24 September 2013, Revised 9 October 2019 by Personal Data Protection Commission of Singapore
- Sample Clauses for Obtaining and Withdrawing Consent, 25 May 2015 by Personal Data Protection Commission of Singapore
- Singapore Code of Banking Practices – The Personal Data Protection Act ("PDPA") by The Association of Banks in Singapore (ABS)
- Guide to Developing a Data Protection Management Programme, Published 1 November 2017, Revised 15 July 2019 by Personal Data Protection Commission of Singapore
- Data Classification Secure Cloud Adoption, June 2018 by Amazon Web Services (AWS)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

17. Appendix A

1. Product: Saving Accounts



<u>Product: Saving Account Process Flows</u>

Process 1: กระบวนการพัฒนาผลิตภัณฑ์ (Marketing and Product Development)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- Front office ของธนาคารทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากลูกค้าที่แจ้งความประสงค์ในการเปิดบัญชีกับธนาคารที่สาขา
- แผนกการตลาดหรือแผนกพัฒนาผลิตภัณฑ์ของธนาคารทำการเก็บรวบรวมข้อมูลจากการให้ลูกค้าทำการกรอกแบบฟอร์มการสำรวจความพึงพอใจ ทั้งแบบออนไลน์ เช่น ผ่านทางเว็บไซต์ หรือ แบบออฟไลน์ เช่น การเก็บข้อมูลจากสาขาของธนาคาร

การใช้ข้อมูล (Use)

- แผนกการตลาดหรือแผนกพัฒนาผลิตภัณฑ์ ใช้ข้อมูลส่วนบุคคลเพื่อใช้ในการทำวิจัยและพัฒนาผลิตภัณฑ์ รวมถึงวิเคราะห์พฤติกรรมของลูกค้าเพื่อการสร้าง Product Program และส่งไปที่ คณะกรรมการบริหารสินทรัพย์และหนี้สิน (Asset and Liability Management Committee : ALCO) เพื่อตรวจทานและอนุมัติการออก Product Program
- Front office นำส่งข้อมูลไปยังแผนกการตลาดหรือแผนกพัฒนาผลิตภัณฑ์ เพื่อใช้ข้อมูลที่ได้จากแบบสำรวจในการวิเคราะห์ความพึงพอใจของลูกค้า เพื่อนำไปปรับปรุงการให้บริการแก่ลูกค้าหรือเพื่อนำไปพัฒนาผลิตภัณฑ์หรือบริการใหม่ให้ตรงกับความต้องการของลูกค้ามากขึ้น

การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร

- แผนกการตลาดหรือแผนกพัฒนาผลิตภัณฑ์ มีการส่งข้อมูล ความพึงพอใจของลูกค้าไปให้แผนกการขายเพื่อใช้ในการนำเสนอผลิตภัณฑ์หรือบริการประเภทเดียวกันหรือผลิตภัณฑ์อื่นของธนาคาร เพื่อให้ตรงกับความต้องการของลูกค้ามากขึ้น

การจัดเก็บข้อมูล (Storage)

- แผนกการตลาดมีการเก็บเอกสารที่ได้รับจากการกรอกแบบสำรวจความพึงพอใจของลูกค้า (Hard Copy) และมีการสแกนเก็บไว้ในระบบของธนาคาร (Soft file) เช่น เก็บในระบบหลักของธนาคาร (Core Banking System : CBS)
- มีการเก็บเอกสารในรูปแบบขอหนังสือหรือสำเนา (Hard Copy) ที่ได้รับจากลูกค้าไว้ในคลังเอกสาร ตามระยะเวลาที่กำหนดในนโยบายของธนาคาร เช่น 10 ปี หลังจากที่ลูกค้าสิ้นสุดความสัมพันธ์ทางธุรกิจกับธนาคาร
- มีการเก็บข้อมูลในรูปแบบของไฟล์อิเล็กทรอนิกส์ (Soft file) ในระบบหลักของธนาคารหรือระบบที่เกี่ยวข้อง (Relational Database) เป็นเวลาที่กำหนดในนโยบายของธนาคาร เช่น 10 ปี หลังจากที่ลูกค้าสิ้นสุดความสัมพันธ์ทางธุรกิจกับธนาคาร

Process 2: การขอเปิดบัญชีออมทรัพย์ (Request for Open Saving Account)

การเก็บรวบรวมข้อมูล (Collection)

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่สาขาของธนาคาร เพื่อการเปิดบัญชีออมทรัพย์ เช่น สำเนาบัตรประชาชน, ชื่อ นามสกุล, เลขบัตรประจำตัวประชาชน, ที่อยู่, ทะเบียนบ้าน, รูปถ่าย, และ ลายเซ็น เป็นต้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

การใช้ข้อมูล (Use)

- Front office ทำการใช้ข้อมูลเพื่อยืนยันตัวตนของลูกค้ากับฐานข้อมูลของธนาคาร เพื่อตรวจสอบว่าลูกค้าคนดังกล่าวเคยเป็นลูกค้าของธนาคารหรือไม่
- Front office ทำการใช้ข้อมูลเพื่อยืนยันตัวตนและตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (KYC, CDD) ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน
- Front office ทำการเทียบข้อมูลยืนยันตัวตนของลูกค้ากับรายชื่อของบุคคลที่ต้องเฝ้าระวัง

Process 3: การอนุมัติการขอเปิดบัญชีออมทรัพย์ (Open Saving Account Approval /Saving Transaction Approval)

การใช้ข้อมูล (Use)

- Front office ทำการส่งข้อมูลส่วนบุคคลของลูกค้าที่ผ่านการตรวจสอบตามข้อกำหนดของกฎหมาย ไปยังผู้ได้รับอนุญาต (Authorized person) เช่น หัวหน้าแผนกเงินฝาก เพื่อทำการขออนุมัติการเปิดบัญชีออมทรัพย์

การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร

- Front office ทำการส่งต่อข้อมูลส่วนบุคคลของลูกค้าภายในแผนก และส่งไปยังหัวหน้าแผนกเพื่อทำการขออนุมัติการเปิดบัญชีออมทรัพย์

Process 4: การจัดเตรียมเพื่อยืนยันการฝากเงินของลูกค้า Prepare Deposit Confirmation for the Customer

- ไม่มีกิจกรรมการประมวลผลข้อมูลส่วนตัวของลูกค้าในกิจกรรมนี้

Process 5: การเก็บเอกสาร (Document Keeping)

การเก็บรักษาข้อมูล (Retention)

- มีการเก็บเอกสารในรูปแบบขอหนังสือหรือสำเนา (Hard Copy) ที่ได้รับจากลูกค้าไว้ในคลังเอกสารของธนาคาร หรือจัดจ้างบริษัทจัดเก็บภายนอก ตามระยะเวลาที่กำหนดในนโยบายของธนาคาร เช่น 10 ปี หลังจากที่ลูกค้าสิ้นสุดความสัมพันธ์ทางธุรกิจกับธนาคาร

- มีการเก็บข้อมูลในรูปแบบของไฟล์อิเล็กทรอนิกส์ (Soft file) ในระบบหลักของธนาคารหรือระบบที่เกี่ยวข้อง (Relational Database) เป็นเวลาที่กำหนดในนโยบายของธนาคาร เช่น 10 ปี หลังจากที่ลูกค้าสิ้นสุดความสัมพันธ์ทางธุรกิจกับธนาคาร

Process 6: การลงบันทึกประวัติของการทำธุรกรรม (Record the Transaction)

<u>การใช้ข้อมูล (Use)</u>

- ข้อมูลทางการเงินของลูกค้า เช่น หมายเลขบัญชี รายงานข้อมูลการเบิก/ถอนเงินในบัญชี ยอดเงินฝากที่มีกับธนาคาร ถูกบันทึกในระบบโดยอัตโนมัติ

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- ข้อมูลที่อยู่ในระบบ CBS พนักงานธนาคารสามารถเข้าถึงได้ ตามสิทธิและหน้าที่ในการปฏิบัติงาน ซึ่งเป็นไปตามนโยบายของธนาคาร ผู้ที่มีอำนาจในการกำหนดสิทธิดังกล่าว จะต้องคำนึงถึงความจำเป็นในการใช้ข้อมูลเพื่อให้การเข้าถึงข้อมูลนั้นเป็นไปตามหลัก Confidentiality
- สำหรับข้อมูลในการบันทึกบัญชีจะถูกเปิดเผยให้กับแผนกบัญชีเพื่อบันทึกข้อมูลลงในระบบ สิทธิในการเข้าถึงและแก้ไขข้อมูลในระบบบัญชีให้เป็นไปตามนโยบายของธนาคาร

Process 7: การคำนวณค่าใช้จ่ายดอกเบี้ย (Interest Expense Calculation)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- Sales & Marketing/Front Office ทำการเก็บรวบรวมผลิตภัณฑ์ที่ลูกค้าเลือก

<u>การใช้ข้อมูล (Use)</u>

- ข้อมูลเงื่อนไขของผลิตภัณฑ์ที่ลูกค้าเลือกจะถูก Configure ระบบบัญชีเพื่อทำการคำนวณค่าใช้จ่ายดอกเบี้ยรายวันโดยอัตโนมัติ

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- แผนกบัญชีได้รับข้อมูลเพื่อบันทึกค่าใช้จ่ายดอกเบี้ยลงในระบบของธนาคาร

<u>การจัดเก็บข้อมูล (Storage)</u>

- แผนกบัญชีทำการจัดเก็บข้อมูลทางธุรกรรมในส่วนของดอกเบี้ยลงในระบบของธนาคาร

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

Process 8: การถอนเงิน/ปิดบัญชีกับธนาคาร (Request for Withdrawal/Closing Account)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- บนช่องทางออนไลน์ มีการเก็บรวบรวมข้อมูล เช่น หมายเลขรหัสประจำตัว (PIN), ลายนิ้วมือ, และ ข้อมูลการยืนยันตัวตนด้วยการสแกนใบหน้า
- ในช่องทางของสาขาธนาคาร มีการเก็บรวบรวมข้อมูล เช่น สมุดเงินฝาก และ บัตรประจำตัวประชาชนของลูกค้า

<u>การใช้ข้อมูล (Use)</u>

- ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมจากช่องทางออนไลน์นำมาใช้ในการยืนยันตัวตนของลูกค้า และอนุมัติการถอนเงินจากบัญชี หรือทำการปิดบัญชี
- ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมจากช่องทางสาขานำมาใช้ในการยืนยันตัวตนของลูกค้า และอนุมัติการถอนเงินจากบัญชี หรือทำการปิดบัญชี

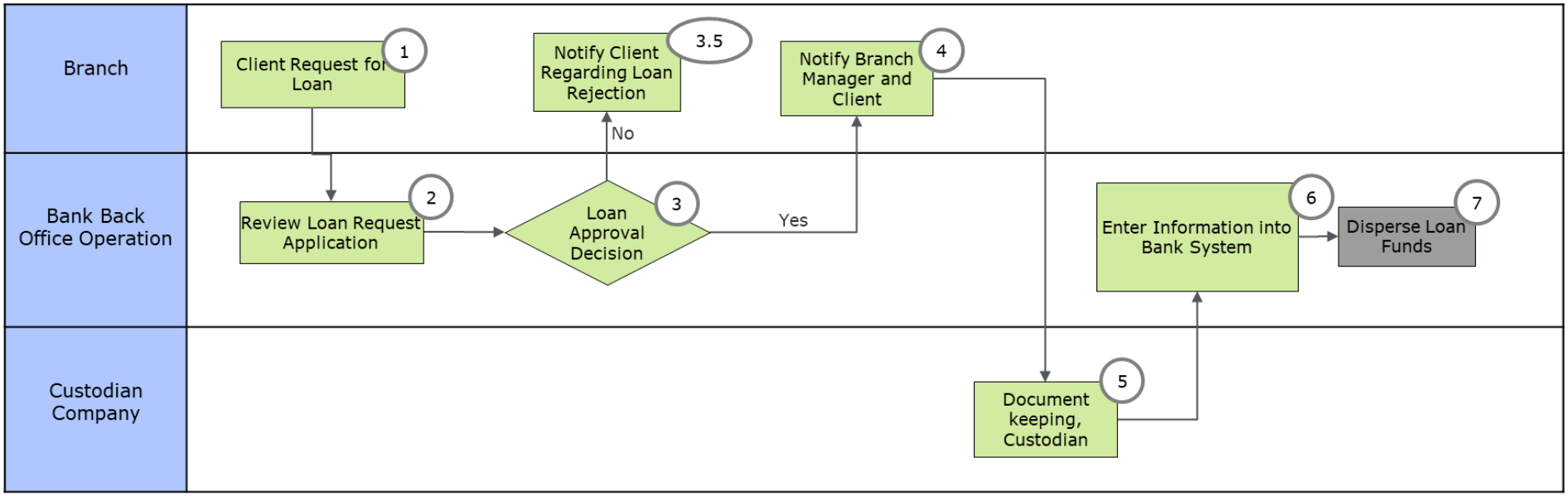
<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- แผนกบัญชีได้รับข้อมูลจากแผนก Front Office หรือจากช่องทางออนไลน์ เพื่อทำการบันทึกรายการถอนเงินหรือ รายการปิดบัญชีลงในระบบของธนาคาร

<u>การจัดเก็บข้อมูล (Storage)</u>

- แผนกบัญชีมีการเก็บบันทึกรายการการทำธุรกรรมรายการการฝาก ถอนเงินหรือปิดบัญชี ไว้ในระบบของธนาคารเป็นเวลา 10 ปีนับจากสิ้นสุดความสัมพันธ์ทางธุรกิจกับลูกค้าหรือตามที่นโยบายของธนาคารกำหนด

2. Product: Loan Process



<u>Product: Loan Process</u>

Process 1: ลูกค้ายื่นความประสงค์ในการขอสินเชื่อ (Client Request for a Loan)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากลูกค้าที่แจ้งความประสงค์ในการขอสินเชื่อกับธนาคารที่สาขา ข้อมูลที่ธนาคารทำการเก็บรวบรวม เช่น ชื่อ นามสกุล ข้อมูลอาชีพ ข้อมูลรายได้ ประวัติครอบครัว ข้อมูลคู่สมรส เป็นต้น

<u>การใช้ข้อมูล (Use)</u>

- ธนาคารใช้ข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ในการขอสินเชื่อกับธนาคาร

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

- สาขามีการส่งข้อมูลลูกค้าและแบบฟอร์มการยื่นขอสินเชื่อต่อไปยัง back office operation เพื่อเข้าสู่กระบวนการวิเคราะห์สินเชื่อ

<u>การจัดเก็บข้อมูล (Storage)</u>

- สาขามีการเก็บเอกสารประกอบการขอสินเชื่อที่ได้รับจากลูกค้าทั้งในรูปแบบสำเนาเอกสาร (Hard Copy) และในรูปแบบของอิเล็กทรอนิกส์ไฟล์ (Soft file) จากการสแกนเก็บไว้ในระบบของธนาคาร

Process 2: ธนาคารตรวจสอบคำร้องขอสินเชื่อ (Review Loan Request Application)

<u>การใช้ข้อมูล (Use)</u>

- Back Office Operation นำข้อมูลส่วนบุคคลของลูกค้าที่แจ้งความประสงค์ในการขอสินเชื่อ เพื่อยืนยันตัวตนของลูกค้า (Identity Verification) และ เพื่อตรวจสอบความถูกต้องและครบถ้วนของแบบฟอร์มการขอสินเชื่อ

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- มีการส่งข้อมูลส่วนบุคคลที่อยู่ในรูปแบบสำเนาเอกสาร (Hard Copy) และในรูปแบบของอิเล็กทรอนิกส์ไฟล์ (Soft file) เพื่อแจ้งความประสงค์ในการขอสินเชื่อ ต่อไปให้ทีมบริหารความเสี่ยง (Risk Management) เพื่อทำการวิเคราะห์สินเชื่อและพิจารณาการอนุมัติสินเชื่อต่อไป

Process 3: ธนาคารอนุมัติ/ปฏิเสธ คำร้องขอสินเชื่อ (Loan Approval Decision) และ Process 3.5: แจ้งต่อลูกค้า ในกรณีที่ธนาคารปฏิเสธคำร้องขอสินเชื่อ (Notify Client Regarding Loan Rejection)

<u>การใช้ข้อมูล (Use)</u>

- ทีม Risk Management นำข้อมูลส่วนบุคคลมาเพื่อประเมินความเสี่ยงของผู้กู้ ความสามารถในการจ่ายชำระ เพื่อประกอบการพิจารณาการอนุมัติสินเชื่อ

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- มีการส่งข้อมูลส่วนบุคคลรวมทั้งผลการวิเคราะห์ข้อมูลเครดิตของลูกค้าไปยัง Underwriter เพื่อทำการเซ็นต์อนุมัติหรือปฏิเสธการให้สินเชื่อ และแชร์ข้อมูลกลับไปยัง Relationship manager ของสาขาที่ทำการรับลูกค้าเพื่อทำการแจ้งผลการขอสินเชื่อกับลูกค้า และเพื่อการดำเนินการในขั้นต่อไป

<u>การจัดเก็บข้อมูล (Storage)</u>

- แผนก Risk Management มีการเก็บบันทึกคำขอสินเชื่อ ผลการวิเคราะห์ข้อมูลเครดิต รวมทั้งผลการอนุมัติหรือปฏิเสธการให้สินเชื่อในระบบของธนาคาร

Process 4: แจ้งต่อผู้จัดการสาขาและลูกค้า ในกรณีที่ธนาคารอนุมัติคำร้องขอสินเชื่อ (Notify Branch Manager and Client of Loan Approval)

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในหรือภายนอกธนาคาร</u>

- สาขาธนาคารส่งเอกสารที่เกี่ยวกับการขอสินเชื่อ ซึ่งมีข้อมูลส่วนบุคคลและเป็นเอกสารที่มีผลทางกฎหมายให้ฝ่ายงานที่ทำหน้าที่ในการเก็บเอกสารหรือจัดจ้างหน่วยงานภายนอก เพื่อทำการเก็บรักษาตามขั้นตอนการดำเนินงานของธนาคาร

<u>การจัดเก็บข้อมูล (Storage)</u>

- Relationship manager ของสาขาและแผนกที่เกี่ยวข้องในการดำเนินการขอสินเชื่อ ทำการจัดเก็บข้อมูลส่วนบุคคลของลูกค้า เช่น คำร้องขอสินเชื่อ ผลการอนุมัติสินเชื่อและเอกสารประกอบการขอสินเชื่อ
- สาขาธนาคารส่งเอกสารที่เกี่ยวกับการขอสินเชื่อ ซึ่งมีข้อมูลส่วนบุคคลและเป็นเอกสารที่มีผลทางกฎหมายให้แผนกที่รับผิดชอบ หรือจัดจ้างหน่วยงานภายนอก เพื่อทำการจัดเก็บตามขั้นตอนการดำเนินงานของธนาคาร

Process 5: การเก็บเอกสาร (Document keeping, Custodian)

<u>การจัดเก็บข้อมูล (Storage)</u>

- ผู้ที่ทำหน้าทำหน้าที่ในการจัดเก็บเอกสาร ของสาขามีการจัดเก็บข้อมูลแบ่งตามประเภท ในส่วนของเอกสารต้นฉบับที่ได้รับมามีการจัดเก็บไว้ในห้องเก็บมั่นคง หากเป็นเอกสารประเภทสำเนาอิเล็กทรอนิกส์ทางแผนก Risk Management จะมีการบันทึกและจัดเก็บไว้ในระบบของธนาคารตั้งแต่ขั้นตอนการอนุมัติสินเชื่อ

<u>การเก็บรักษาข้อมูล (Retention)</u>

- ข้อมูลส่วนตัวของลูกค้าทั้งในรูปแบบของเอกสารต้นฉบับหรือสำเนา (Hard Copy) และในรูปแบบของไฟล์อิเล็กทรอนิกส์ (Soft file) มีระยะเวลาในการเก็บรักษา 10 ปีนับตั้งแต่ลูกค้าสิ้นสุดความสัมพันธ์ทางธุรกิจกับธนาคารหรือตามที่นโยบายของธนาคารกำหนด

Process 6: การลงบันทึกประวัติของการทำธุรกรรม (Enter Information into Bank System)

<u>การใช้ข้อมูล (Use)</u>

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

- ข้อมูลส่วนบุคคลของลูกค้าถูกบันทึกในระบบของธนาคาร

<u>การจัดเก็บข้อมูล (Storage)</u>

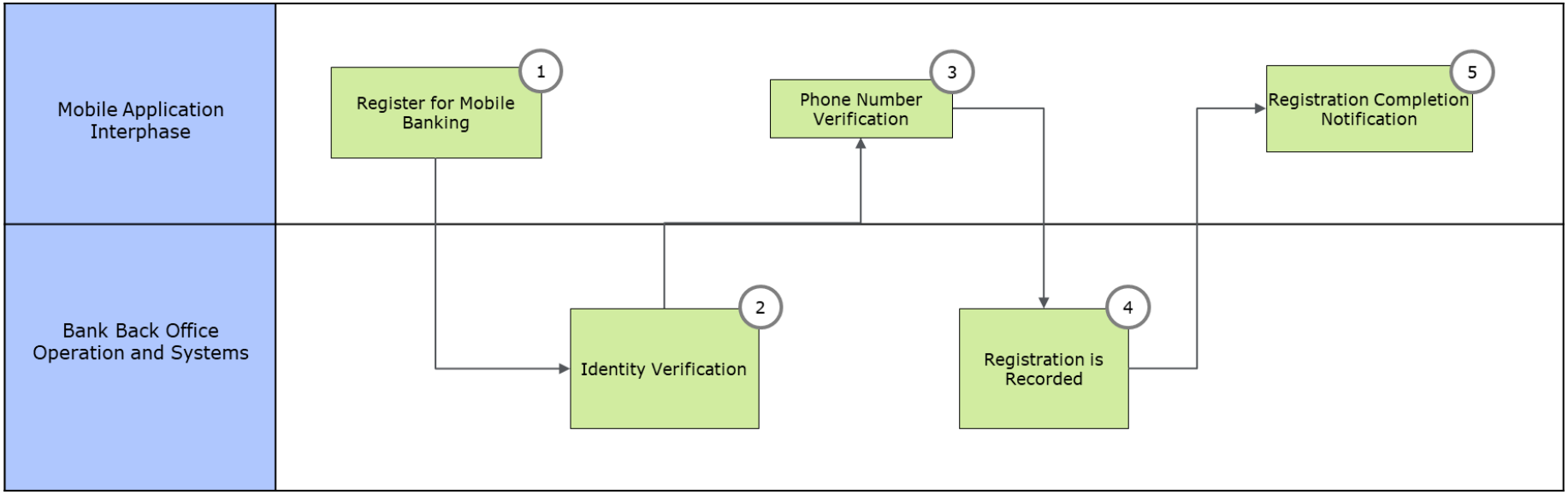
- ข้อมูลการทำธุรกรรมของลูกค้าถูกจัดเก็บในระบบของธนาคาร

Process 7: การโอนสินเชื่อเข้าบัญชีลูกค้า (Disperse Loan Funds)

<u>การใช้ข้อมูล (Use)</u>

- ข้อมูลส่วนบุคคลของลูกค้าถูกใช้เพื่อให้ธนาคารโอนเงินให้กู้ยืมแก่ลูกค้า

3. Product: Mobile Banking (Registration Process)



Product: Mobile Banking

Process 1: การขอสมัครใช้งานแอปพลิเคชัน (Register for Mobile Banking)

การเก็บรวบรวมข้อมูล (Collection)

มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากลูกค้า เช่น ชื่อ นามสกุล หมายเลขเลขบัตรประจำตัวประชาชน

การใช้ข้อมูล (Usage)

- ข้อมูลส่วนบุคคลของลูกค้าจะถูกใช้เพื่อแจ้งความประสงค์ในการขอสมัครใช้งาน Mobile Banking Application ของธนาคาร
- ข้อมูลส่วนบุคคลของลูกค้าที่ใช้ในการสมัครถูกบันทึกเข้าระบบของ Mobile Banking

การจัดเก็บข้อมูล (Storage)

- ข้อมูลส่วนบุคคลของลูกค้าที่ใช้ในการสมัครถูกบันทึกเข้าระบบของ Mobile Banking Application และถูกจัดเก็บในฐานข้อมูลของธนาคาร

Process 2: ธนาคารยืนยันตัวตนลูกค้า (Identity Verification)

การเก็บรวบรวมข้อมูล (Collection)

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่สมัครใช้ Mobile Banking จากฐานข้อมูลของธนาคาร

การใช้ข้อมูล (Use)

- ระบบนำข้อมูลส่วนบุคคลของลูกค้าที่สมัครใช้ Mobile Banking เพื่อยืนยันตัวตนของลูกค้า (Identity Verification)

การจัดเก็บข้อมูล (Storage)

- มีการบันทึกประวัติการสมัครเข้าใช้งาน Mobile Banking ลงไว้ในระบบฐานข้อมูลของธนาคาร

Process 3: ลูกค้ายืนยันตัวตนโดยหมายเลขโทรศัพท์มือถือ (Phone Number Verification)

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

การใช้ข้อมูล (Use)

- ระบบใช้หมายเลขโทรศัพท์ของลูกค้าที่ลงทะเบียนไว้กับหมายเลขบัญชีเพื่อการดำเนินการยืนยันตัวตนโดยหมายเลขโทรศัพท์มือถือ

Process 4: ประวัติการลงทะเบียนถูกจดบันทึกลงในระบบ (Registration is Recorded)

การใช้ข้อมูล (Use)

- ใช้ข้อมูลเพื่อเปิดการใช้งาน Mobile Banking Application

การจัดเก็บข้อมูล (Storage)

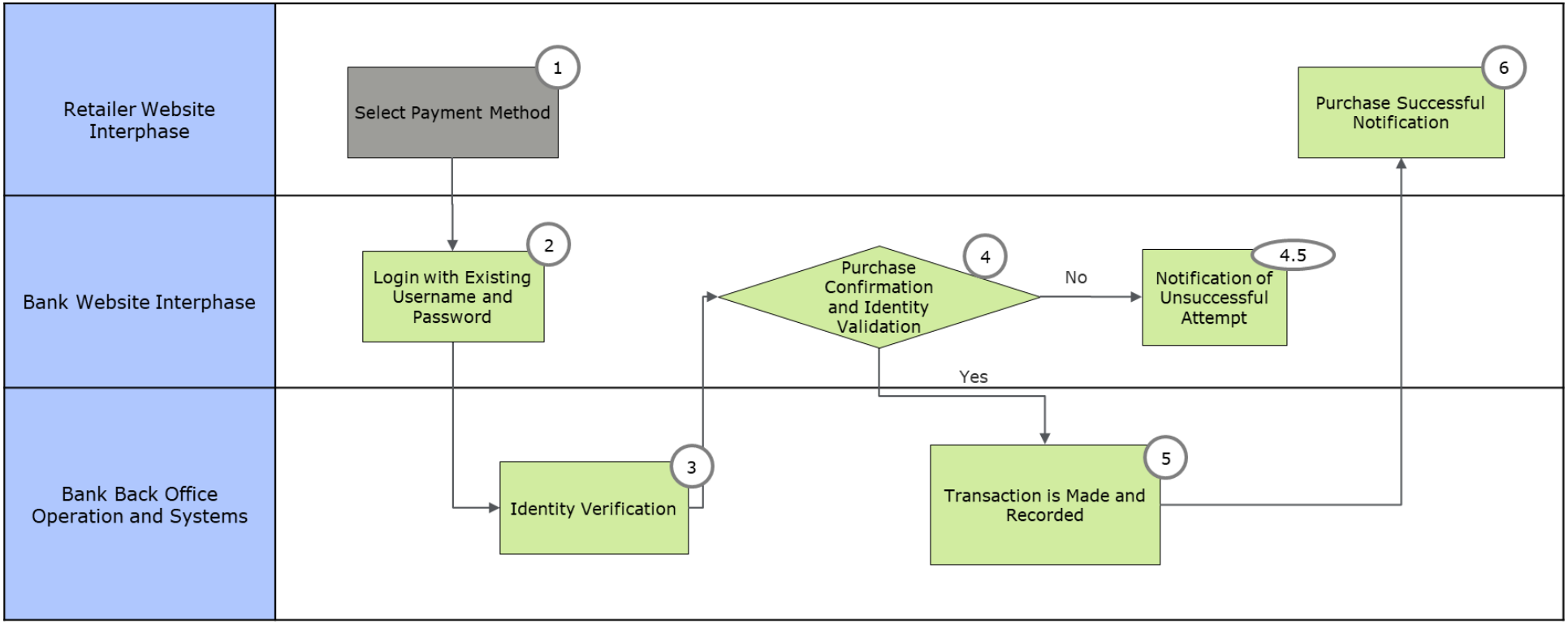
- ระบบ Mobile Banking Application ทำการจัดเก็บข้อมูลส่วนบุคคลจากการขอใช้งานระบบ และข้อมูลส่วนบุคคลจะถูกจัดเก็บในฐานข้อมูลของธนาคารต่อไป

Process 5: แจ้งลูกค้าว่าการลงทะเบียนเสร็จสมบูรณ์ (Registration Completion Notification)

การใช้ข้อมูล (Use)

- ระบบแจ้งว่าขั้นตอนการลงทะเบียนเสร็จสมบูรณ์แก่ลูกค้าบนหน้าของแอปพลิเคชัน

4. Service: Internet Banking (Purchase Product Process)



<u>Product: Internet Banking</u>

Process 1: ลูกค้าเลือกวิธีชำระเงิน (Select Payment Method)

- ไม่มีกิจกรรมการประมวลผลข้อมูลส่วนตัวของลูกค้าในกิจกรรมนี้

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

Process 2: ลูกค้าล็อกอินเข้าระบบ Internet Banking (Login with Existing Username and Password)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากลูกค้าที่ลงทะเบียนเข้าสู่ระบบ Internet Banking

<u>การเปิดเผยข้อมูล (Disclosure) – ไปยังบุคคลที่สาม</u>

- ข้อมูลส่วนบุคคลของลูกค้ารวมถึงยอดที่ต้องชำระ ถูกส่งมาจากระบบเว็บไซต์ของร้านค้า หรือ ผู้ให้บริการ

<u>การจัดเก็บข้อมูล (Storage)</u>

- ระบบ Internet Banking ทำการเก็บประวัติการลงทะเบียนเข้าสู่ระบบของลูกค้า

Process 3: ธนาคารยืนยันตัวตันลูกค้า (Identity Verification)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่ลงทะเบียนเข้าสู่ระบบ Internet Banking และ ข้อมูลส่วนบุคคลของลูกค้าจากระบบของธนาคาร

<u>การใช้ข้อมูล (Use)</u>

- ระบบนำข้อมูลส่วนบุคคลของลูกค้าที่ลงทะเบียนเข้าสู่ระบบ Internet Banking และ ข้อมูลส่วนบุคคลของลูกค้าจากระบบของธนาคาร เพื่อยืนยันตัวตนของลูกค้า (Identity Verification)

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- ข้อมูลส่วนบุคคลของลูกค้าที่ลงทะเบียนเข้าสู่ระบบ Internet Banking ถูกส่งต่อไปยังระบบของธนาคาร

Process 4: ลูกค้ายืนยันการสั่งซื้อ และยืนยันตัวตนโดยหมายเลขโทรศัพท์มือถือ (Purchase Confirmation and Identity Validation)

<u>การใช้ข้อมูล (Use)</u>

- ระบบใช้หมายเลขโทรศัพท์มือถือของลูกค้าที่ลงทะเบียนไว้กับหมายเลขบัญชีเพื่อการดำเนินการยืนยันตัวตนโดยหมายเลขโทรศัพท์มือถือ

<u>การจัดเก็บข้อมูล (Storage)</u>

- ระบบบันทึกประวัติการยืนยันตัวตนด้วยหมายเลขโทรศัพท์มือถือของลูกค้า

Process 4.5: แจ้งต่อลูกค้า ในกรณีที่ยืนยันตัวตนไม่สำเร็จ (Notification of Unsuccessful Attempt)

<u>การใช้ข้อมูล (Use)</u>

- ระบบแจ้งแก่ลูกค้าในกรณีที่ยืนยันตัวตนไม่สำเร็จ รวมถึงเหตุผล เช่น ลูกค้าใส่ Username หรือ Password ผิด เป็นต้น

Process 5: การลงบันทึกประวัติของการทำธุรกรรม (Transaction is Made and Recorded)

<u>การใช้ข้อมูล (Use)</u>

- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อบันทึกประวัติการทำธุรกรรม
- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อดำเนินการหักยอดที่ชำระจากบัญชีของลูกค้า และโอนยอดที่ถูกชำระเข้าบัญชีของร้านค้าหรือผู้ให้บริการ

<u>การจัดเก็บข้อมูล (Storage)</u>

- ประวัติการทำธุรกรรมถูกบันทึกลงในระบบของธนาคาร

Process 6: แจ้งต่อลูกค้าว่าคำสั่งซื้อสำเร็จครบถ้วน (Purchase Successful Notification)

<u>การใช้ข้อมูล (Use)</u>

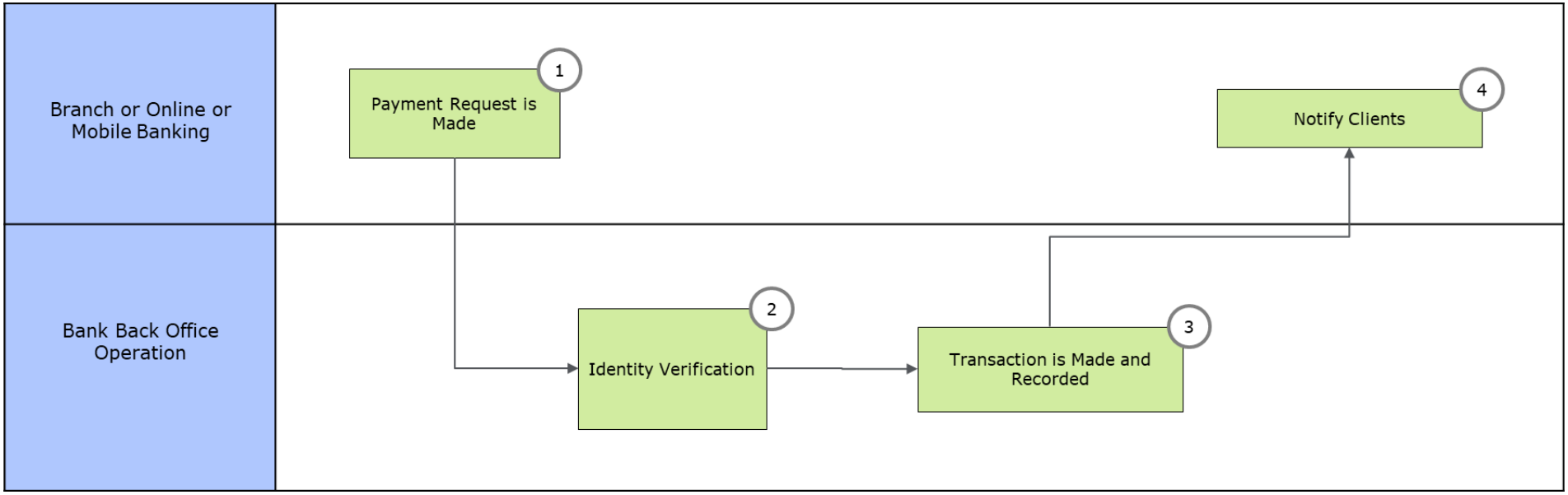
- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อแจ้งแก่ลูกค้าถึงยอดที่ชำระเสร็จสิ้น

<u>การเปิดเผยข้อมูล (Disclosure) – ไปยังบุคคลที่สาม</u>

- ข้อมูลส่วนบุคคลของลูกค้ารวมถึงยอดที่ชำระเสร็จสิ้น ถูกส่งไปยังระบบเว็บไซต์ของร้านค้าหรือผู้ให้บริการ

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

5. Product: Payment



Process 1: ลูกค้ายื่นความจำนงในการขอชำระค่าสินค้าหรือบริการ (Payment Request is Made)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากลูกค้าที่แจ้งความประสงค์ในการขอชำระค่าสินค้าหรือบริการ

<u>การเปิดเผยข้อมูล (Disclosure) – ภายในธนาคาร</u>

- สาขาหรือ Internet/Mobile Banking มีการส่งข้อมูลลูกค้าและยอดบิลที่ลูกค้าต้องการชำระไปยัง back office operation
- สาขา/หรือ ระบบ Internet/Mobile Banking มีการส่งข้อมูลส่วนบุคคลของลูกค้าเพื่อเก็บลงในระบบของธนาคาร

Process 2: ธนาคารยืนยันตัวตนของลูกค้า (Identity Verification)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่ในการขอชำระค่าสินค้าหรือบริการ จากระบบของธนาคาร เช่น ชื่อ สกุล หมายเลขบัตรประชาชน เป็นต้น

<u>การใช้ข้อมูล (Use)</u>

- ระบบของธนาคาร นำข้อมูลส่วนบุคคลของลูกค้าที่แจ้งความจำนงในการขอชำระค่าสินค้าหรือบริการ เพื่อยืนยันตัวตนของลูกค้า (Identity Verification)

Process 3: การลงบันทึกประวัติของการทำธุรกรรม (Transaction is Made and Recorded)

<u>การใช้ข้อมูล (Use)</u>

- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อบันทึกประวัติการทำธุรกรรม
- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อดำเนินการหักยอดที่ชำระจากบัญชีของลูกค้า และโอนยอดที่ถูกชำระเข้าบัญชีของร้านค้าหรือผู้ให้บริการ

<u>การจัดเก็บข้อมูล (Storage)</u>

- ประวัติการทำธุรกรรมถูกบันทึกลงในระบบของธนาคาร

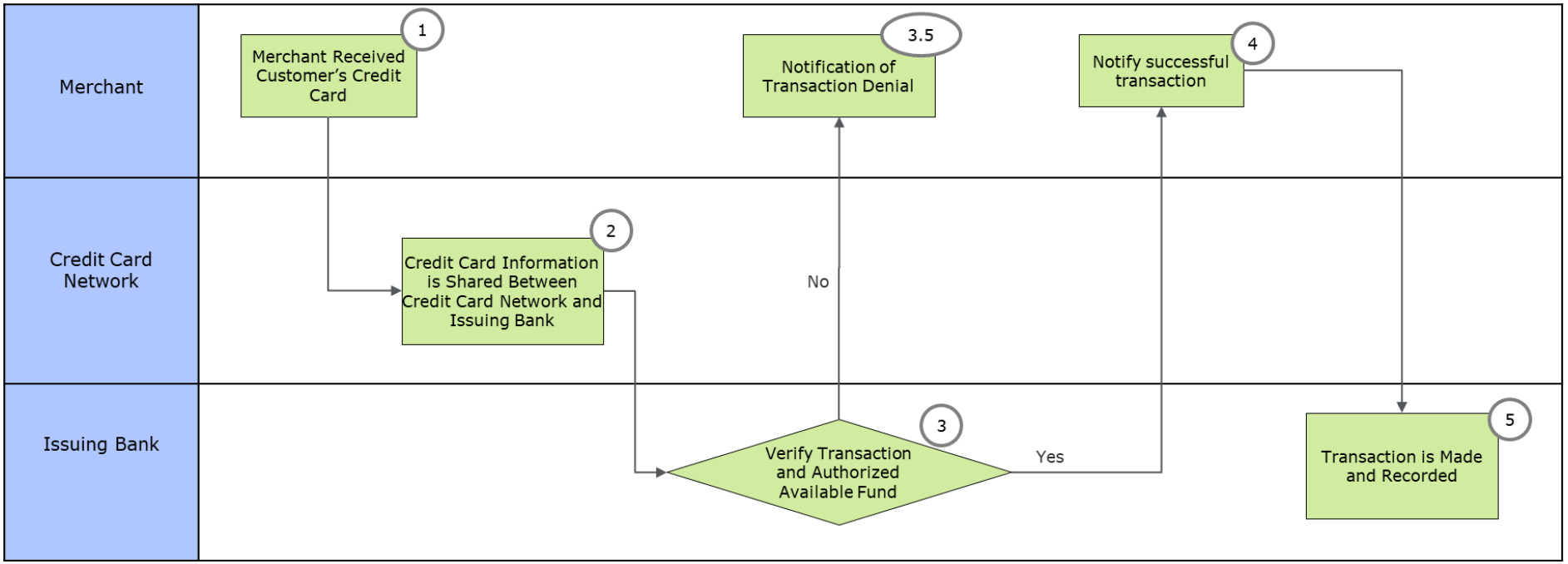
Process 4: แจ้งต่อลูกค้าว่าการทำธุรกรรมเสร็จสิ้น (Notify Client)

<u>การใช้ข้อมูล (Use)</u>

- ระบบหรือ สาขา ใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อแจ้งแก่ลูกค้าถึงยอดที่ชำระเสร็จสิ้น

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

6. Product: Credit Card



Process 1: ร้านค้ารับบัตรเครดิตของลูกค้าเพื่อชำระค่าสินค้าหรือบริการ (Merchant Received Customer's Credit Card)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากบัตรเครดิตของลูกค้า

<u>การเปิดเผยข้อมูล (Disclosure) – ไปยังบุคคลที่สาม</u>

- ระบบเครื่องรูดบัตรเครดิตส่งข้อมูลส่วนบุคคลของลูกค้าต่อไปยัง Credit Card Network

Process 2: ธนาคารยืนยันตัวตนของลูกค้า (Credit Card Information is shared between Credit Card Network and Issuing Bank)

<u>การเปิดเผยข้อมูล (Disclosure) – ไปยังบุคคลที่สาม</u>

- ระบบของ Credit Card Network ส่งต่อข้อมูลบัตรเครดิตและข้อมูลส่วนบุคคลของลูกค้าไปยังธนาคารผู้ออกบัตร

Process 3: ธนาคารยืนยันธุรกรรม และ อนุมัติยอดชำระ (Verify Transaction and Authorized Available Fund)

<u>การเก็บรวบรวมข้อมูล (Collection)</u>

- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าจาก Credit Card Network
- มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าจากระบบของธนาคาร

<u>การใช้ข้อมูล (Use)</u>

- ระบบนำข้อมูลส่วนบุคคลของลูกค้าจาก Credit Card Network เพื่อนำมายืนยันตัวตนกับ ข้อมูลส่วนบุคคลของลูกค้าจากระบบของธนาคาร
- ใช้ข้อมูลเพื่ออนุมัติยอดชำระ จากวงเงินที่มีอยู่ของบัตรเครดิตลูกค้า

Process 3.5: แจ้งต่อลูกค้า ในกรณีที่ธุรกรรมไม่ได้รับการอนุมัติ (Notification of Transaction Denial)

<u>การใช้ข้อมูล (Use)</u>

- ระบบแจ้งแก่ลูกค้าในกรณีที่ธุรกรรมไม่ได้รับการอนุมัติ รวมถึงเหตุผล เช่น วงเงินบัตรเครดิตเต็มเป็นต้น

<u>การแชร์ข้อมูล (Share)</u>

- ส่งข้อมูลของลูกค้ารวมถึงข้อมูลว่าธุรกรรมไม่ได้รับการอนุมัติไปยังระบบชำระเงินของร้านค้า

<u>การจัดเก็บข้อมูล (Storage)</u>

- มีการบันทึกธุรกรรมที่ไม่ได้รับการอนุมัติลงในระบบของธนาคาร

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

Process 4: แจ้งต่อลูกค้าว่าทำธุรกรรมเสร็จสิ้น (Notification of Successful Transaction)

<u>การใช้ข้อมูล (Use)</u>

- ระบบแจ้งแก่ลูกค้าถึงการทำธุรกรรมสำเร็จ และยอดเงินที่ถูกชำระ

<u>การแชร์ข้อมูล (Share)</u>

- ส่งข้อมูลของลูกค้ารวมถึงข้อมูลว่าธุรกรรมได้รับการอนุมัติไปยังระบบชำระเงินของร้านค้า

Process 5: การลงบันทึกประวัติของการทำธุรกรรม (Transaction is Made and Recorded)

<u>การใช้ข้อมูล (Use)</u>

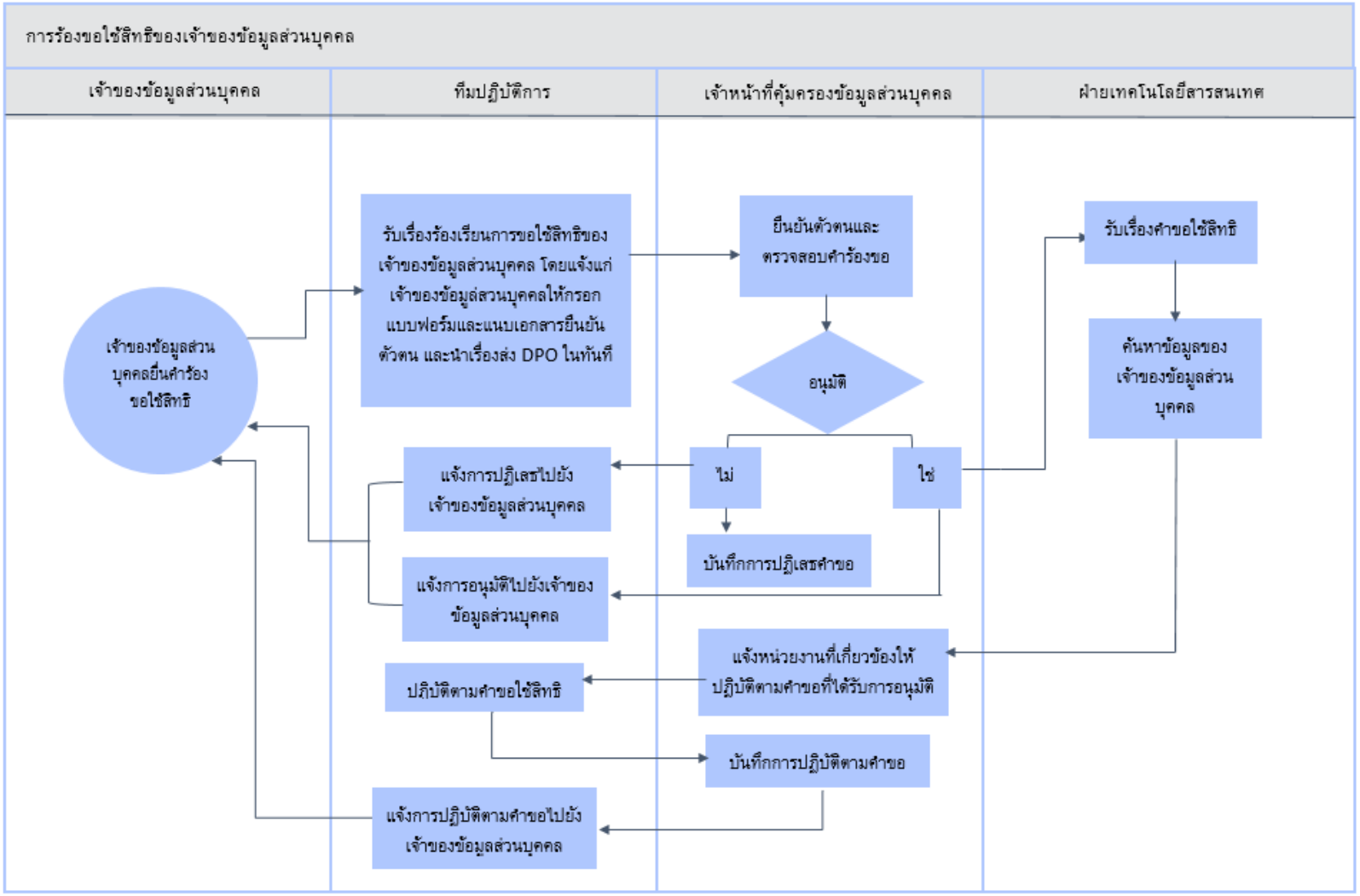
- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อบันทึกประวัติการทำธุรกรรม
- ระบบใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อดำเนินการหักยอดที่ชำระจากวงเงินบัตรเครดิตของลูกค้า และโอนยอดที่ถูกชำระเข้าบัญชีของร้านค้าหรือผู้ให้บริการ

<u>การจัดเก็บข้อมูล (Storage)</u>

- ประวัติการทำธุรกรรมถูกบันทึกลงในระบบของธนาคาร

18. Appendix B

18.1 ตัวอย่างกระบวนการปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล



© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

19. Appendix C

ตัวอย่างแนวทางปฏิบัติการทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้

19.1 การจัดทำข้อมูลนิรนาม (Data Anonymization)

การจัดทำข้อมูลนิรนาม หมายถึง กระบวนการในการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ โดยทั่วไปคำศัพท์ที่ใช้ในแต่ละแหล่งอ้างอิงอาจแตกต่างกันไป ตัวอย่างเช่น บ้างใช้คำว่า การทำข้อมูลนิรนาม (Anonymization) และการขจัดตัวตน (De-Identification)

<u>ตัวอย่างการจัดทำข้อมูลนิรนาม</u>

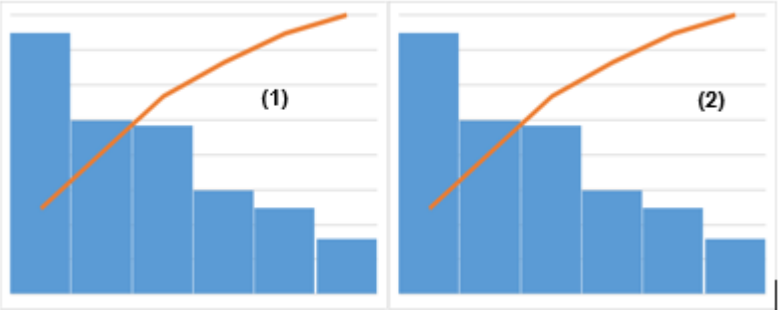
การจัดทำข้อมูลนิรนามสามารถทำได้โดยการเปลี่ยนแปลงข้อมูลต้นฉบับให้เป็นข้อมูลที่ไม่สามารถนำไปประบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้ ก่อนที่จะมีการนำข้อมูลไปประมวลผลตามวัตถุประสงค์ต่างๆของธนาคาร

ชื่อ	อีเมล	แผนก	รายได้-ยอดขาย
สมชาย	Somchai@abc.com	ฝ่ายขาย	500,000
กวิน	Kwin@abc.com	ฝ่ายขาย	970,000
สมปอง	Sompong@abc.com	ฝ่ายขาย	600,000
ปราณี	Pranee@abc.com	ฝ่ายขาย	1,000,000
วิเชียร	Viche@abc.com	ฝ่ายขาย	1,500,000
สมาน	Smarn@abc.com	ฝ่ายขาย	320,000

<u>ข้อมูลต้นฉบับ (1)</u>

ชื่อ	แผนก	รายได้-ยอดขาย
A	ฝ่ายขาย	500,000
B	ฝ่ายขาย	970,000
C	ฝ่ายขาย	600,000
D	ฝ่ายขาย	1,000,000
E	ฝ่ายขาย	1,500,000
F	ฝ่ายขาย	320,000

<u>ข้อมูลที่มีการทำข้อมูลนิรนาม (2)</u>



ผลลัพธ์ของการประมวลผลข้อมูล (1), (2)

การจัดทำข้อมูลนิรนามนั้นธนาคารจะต้องคำนึงถึงความเสี่ยงในการชี้กลับอัตลักษณ์บุคคล (Re-identification) ที่สามารถทำได้ด้วยวิธีการอย่างเช่น

- การนำข้อมูลส่วนบุคคลตั้งต้นซึ่งอาจได้มาจากแหล่งอื่นนำมาค้นหา จับคู่ หรือประมวลผลร่วมกับข้อมูลนิรนามเพื่อให้สามารถชี้กลับอัตลักษณ์บุคคล
- การนำข้อมูลส่วนบุคคลตั้งต้นมาจากแหล่งข้อมูลสาธารณะนำมาค้นหา จับคู่ หรือประมวลผลร่วมกับข้อมูลนิรนามเพื่อให้สามารถชี้กลับอัตลักษณ์บุคคล

ดังนั้นการจัดทำข้อมูลนิรนามควรยึดหลัก Data Minimization เพื่อใช้ข้อมูลเท่าที่จำเป็นและลดความเสี่ยงในการชี้กลับอัตลักษณ์บุคคล

19.2 การแฝงข้อมูล (Data Pseudonymisation)

การแฝงข้อมูล คือการแทนที่สิ่งที่ระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคล ด้วยการอ้างอิงอื่น ๆ ตัวอย่างเช่น การแทนที่ชื่อบุคคล ด้วย รหัสหรือหมายเลขอ้างอิงที่สร้างขึ้นแบบสุ่ม ซึ่งข้อมูลทั้งสองชุดจะต้องถูกลดความสามารถในการเชื่อมโยงกัน เพื่อลดความเสี่ยงในการชี้กลับอัตลักษณ์บุคคล (Re-identification) และผลกระทบจากเหตุการณ์ถูกละเมิดข้อมูล ในความหมายของ GDPR หมายถึง กระบวนการประมวลผลข้อมูลในลักษณะที่ข้อมูลไม่สามารถระบุตัวบุคคลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ข้อมูลเพิ่มเติมอีกชุดควรทำการเก็บรักษาไว้แยกออกจากกัน ไม่ให้เข้าถึงข้อมูลได้ทั้งสองชุดเพื่อลดความสามารถในการเชื่อมโยงข้อมูลดังกล่าวในการกลับไประบุตัวเจ้าของข้อมูลส่วนบุคคลได้

ชื่อ	แผนก	รายได้-ยอดขาย
CTM-001	ฝ่ายขาย	500,000
CTM-002	ฝ่ายขาย	970,000
CTM-003	ฝ่ายขาย	600,000
CTM-004	ฝ่ายขาย	1,000,000
CTM-005	ฝ่ายขาย	1,500,000
CTM-006	ฝ่ายขาย	320,000

ข้อมูลที่มีการทำการแฝงข้อมูล

ชื่อ	คีย์การชี้กลับอัตลักษณ์
สมชาย	CTM-001
กวิน	CTM-002
สมปอง	CTM-003
ปราณี	CTM-004
วิเชียร	CTM-005
สมาน	CTM-006

ข้อมูลประกอบสำหรับการชี้กลับอัตลักษณ์บุคคล

19.3 การเข้ารหัสข้อมูล (Data Encryption)

การเข้ารหัสข้อมูล คือการใช้หลักการการทางคณิตศาสตร์หรือรหัสการเข้าถึง(คีย์)ในการเข้าถึงข้อมูลส่วนบุคคลที่ถูกเข้ารหัส โดยการเข้ารหัสข้อมูลเป็นหนึ่งในวิธีการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันอาชญากรไซเบอร์ ผู้ประสงค์ร้าย หรือผู้ที่ไม่ได้รับอนุญาติไม่ให้เข้าถึงข้อมูลส่วนบุคคลของธนาคาร โดยหลักการการเข้ารหัสข้อมูลนั้นขึ้นอยู่กับนโยบายการรักษาความปลอดภัยข้อมูลของธนาคารในการกำหนดแบบแผนแนวทางการเข้ารหัสเพื่อลดคความเสี่ยงในการถูกละเมิดข้อมูลส่วนบุคคล

โดยการการเข้ารหัสข้อมูลควรบังคับใช้กับข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่ถูกเก็บไว้ในอุปกรณ์จัดเก็บข้อมูล (Encryption for Data Stroage) และข้อมูลส่วนบุคคลที่อยู่ในขณะส่ง (Encryption for Data in transit)

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam. In each of these, operations are conducted by separate and independent legal entities.

About Deloitte Thailand
In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.