ธนาคารแห่งประเทศไทย
BANK OF THAILAND

เอกสารรับฟังความเห็น

“แนวทางการกำกับดูแลให้มีกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลที่อยู่กับภาคสถาบันการเงินได้”

(ภายใต้โครงการ Your Data ส่วนที่อยู่ภายใต้การกำกับ ธปท.)

ฝ่ายกลยุทธ์สถาบันการเงิน
สายนโยบายสถาบันการเงิน
ธนาคารแห่งประเทศไทย
กุมภาพันธ์ 2568

สารบัญ

บทสรุปผู้บริหาร

การเปิดกว้างให้มีการใช้ประโยชน์จากข้อมูล (open data) เป็นหนึ่งในแนวนโยบายสำคัญภายใต้ภูมิทัศน์ใหม่ภาคการเงินไทยด้านการเงินดิจิทัล โดยจะเป็นจุดเปลี่ยนสำคัญที่จะนำไปสู่การพัฒนานวัตกรรมทางการเงินดิจิทัล ซึ่งจะช่วยยกระดับบริการให้มีประสิทธิภาพและตอบโจทย์ความต้องการของผู้ใช้บริการได้ดีขึ้น โดยเฉพาะ **(1) การเข้าถึงสินเชื่อในระบบอย่างเหมาะสม และ (2) การบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล** โดยเฉพาะลูกค้ารายย่อยและผู้ประกอบการรายเล็ก ซึ่งยังเป็นช่องว่างสำคัญในระบบการเงินไทย **ในปัจจุบันข้อมูลของลูกค้ายังอยู่กระจัดกระจายอยู่กับผู้ให้บริการและหน่วยงานต่าง ๆ** ซึ่งหากมีกลไกที่ลูกค้าสามารถขอให้หน่วยงานที่เก็บข้อมูลส่งข้อมูลของตนไปยังหน่วยงานอื่นได้สะดวก ตามสิทธิภายใต้กฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) จะช่วยให้ลูกค้าสามารถใช้ประโยชน์จากข้อมูลของตน เพื่อให้ได้รับบริการทางการเงินที่ดีขึ้นได้

ธนาคารแห่งประเทศไทย (ธปท.) และหน่วยงานที่เกี่ยวข้องจึงได้ร่วมกันในโครงการ “Your Data” ผลักดันกลไกให้ประชาชนสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่ทั้งในและนอกภาคการเงินผ่านช่องทางดิจิทัล เพื่อประโยชน์ในการได้รับบริการทางการเงินที่ตอบโจทย์มากขึ้น โดยในส่วน**ข้อมูลนอกภาคการเงิน** ธปท. อยู่ระหว่างดำเนินการร่วมกับสำนักงานพัฒนารัฐบาลดิจิทัล หน่วยงานสาธารณูปโภคที่เกี่ยวข้อง และกรมสรรพากร ในการพัฒนาช่องทางให้ประชาชนสามารถส่ง***ข้อมูลการใช้และการจ่ายค่าไฟฟ้าและน้ำประปาและข้อมูลแบบภาษี*** ไปให้กับผู้ให้บริการทางการเงินได้ โดยคาดว่าจะเริ่มส่งได้ภายในปี 2568 สำหรับ**ข้อมูลในภาคการเงิน** ธปท. อยู่ระหว่างผลักดันให้ผู้ให้บริการภายใต้การกำกับของ ธปท. จัดทำกลไกที่ลูกค้าสามารถใช้สิทธิส่ง***ข้อมูลเงินฝาก สินเชื่อ และการชำระเงิน*** ไปให้ผู้ให้บริการรายอื่นๆ ทางดิจิทัลได้ นอกจากนี้อยู่ระหว่างร่วมกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ผลักดันในส่วน***ข้อมูลการถือครองหลักทรัพย์และกรมธรรม์ประกันภัย*** และการมีกลไกให้ลูกค้าใช้สิทธิส่งข้อมูลระหว่างผู้ให้บริการในภาคสถาบันการเงินกับผู้ให้บริการในภาคตลาดทุนและภาคประกันภัยได้ **ทั้งนี้ การผลักดันให้เกิดกลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่กับผู้ให้บริการภายใต้การกำกับของ ธปท. ได้นั้น** จำเป็นต้องอาศัยทั้ง (1) การวางกฎกติกา เพื่อกำกับดูแลผู้ให้บริการในการจัดทำกลไกรับส่งข้อมูลทางดิจิทัลที่พร้อมให้ลูกค้าใช้สิทธิได้สะดวก ปลอดภัย ไม่ถูกปิดกั้น และ (2) ผู้ที่เกี่ยวข้องเข้ามามีส่วนร่วมจัดทำมาตรฐานกลางและแนวปฏิบัติในการรับส่งข้อมูล เพื่อให้ใช้งานได้จริง

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อรับความเห็นต่อแนวทางการกำกับดูแลให้ผู้ให้บริการทางการเงินภายใต้การกำกับของ ธปท. จัดทำกลไกให้ลูกค้าใช้สิทธิส่งข้อมูลของตนที่อยู่กับผู้ให้บริการเหล่านี้ได้ เพื่อประโยชน์ในการได้รับบริการทางการเงินที่ตอบโจทย์ได้ดีขึ้น โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสม และการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล โดยมีหลักการและสาระสำคัญ ดังนี้

1. หลักการสำคัญ: ประชาชนซึ่งเป็นเจ้าของข้อมูลมีสิทธิขอให้ผู้ที่เก็บรวบรวมข้อมูลของตนส่งข้อมูลไปยังหน่วยงานอื่นได้ด้วยวิธีการอัตโนมัติ หากผู้ที่เก็บรวบรวมข้อมูลได้จัดทำข้อมูลนั้นให้อยู่ในรูปแบบที่พร้อมนำไป

ประมวลผลต่อและมีระบบรับส่งข้อมูลด้วยวิธีอัตโนมัติไว้รองรับการใช้สิทธิของเจ้าของข้อมูล ธปท. จึงใช้หลักการดังนี้ในการกำหนดให้ผู้ให้บริการภายใต้การกำกับของ ธปท. จัดทำกลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนได้อย่างสะดวก ปลอดภัย ไม่ถูกปิดกั้น

1.1 สิ่งที่อยากเห็น ได้แก่ (1) ผู้ให้บริการทางการเงินที่เก็บข้อมูลที่มีนัยสำคัญต่อลูกค้า ต้องจัดทำข้อมูลและกลไกที่พร้อมให้ลูกค้าใช้สิทธิส่งข้อมูลผ่านช่องทางดิจิทัลได้สะดวก (2) ผู้ให้บริการสามารถได้รับข้อมูลของลูกค้าและนำข้อมูลดังกล่าวไปใช้พัฒนาและนำเสนอบริการทางการเงินที่ตอบโจทย์ (3) การเชื่อมต่อและรับส่งข้อมูล ระหว่างผู้ให้บริการที่รับและส่งข้อมูลต้องเป็นไปตามมาตรฐานกลางและแนวปฏิบัติที่กำหนด เพื่อให้มีประสิทธิภาพและไม่เกิดภาระหรือต้นทุนเกินความจำเป็น

1.2 สิ่งที่ไม่อยากเห็น คือ (1) เงื่อนไขและค่าธรรมเนียม เป็นอุปสรรคต่อการใช้งานและการรับส่งข้อมูลหรือเกิดการเรียกข้อมูลเกินความจำเป็น รวมถึงเกิดการรับข้อมูลเพียงอย่างเดียวโดยไม่ส่งข้อมูลให้ผู้ให้บริการรายอื่น และ (2) ผู้ให้บริการดูแลความเสี่ยงไม่เหมาะสม โดยเฉพาะด้านการรักษาความปลอดภัยข้อมูล ความเป็นส่วนบุคคลของข้อมูล และการคุ้มครองผู้บริโภค

2. สาระสำคัญของแนวทางกำกับดูแลฯ

2.1 ขอบเขตผู้ให้บริการภายใต้การกำกับของ ธปท. ที่ต้องทำกลไกให้พร้อมส่งข้อมูลของลูกค้าทางดิจิทัลเมื่อลูกค้าร้องขอ (ผู้ให้บริการที่ส่งข้อมูล) ต้องครอบคลุมผู้ให้บริการที่เก็บข้อมูลเงินฝาก สินเชื่อ และการชำระเงิน ที่มีนัยสำคัญต่อลูกค้า โดยไม่สร้างภาระหรือต้นทุนเกินความจำเป็นต่อผู้ให้บริการรายเล็กหรือที่ไม่มีความพร้อม เพื่อให้สามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ในการเข้าถึงสินเชื่อในระบบอย่างเหมาะสม และการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล ซึ่งได้แก่ (1) สถาบันการเงินและสถาบันการเงินเฉพาะกิจ (SFIs) ที่ให้บริการเงินฝากแก่ลูกค้าอย่างมีนัยสำคัญ กล่าวคือ การมีจำนวนบัญชีเกินกว่าระดับที่กำหนด (2) ผู้ให้บริการการชำระเงิน ได้แก่ ผู้ให้บริการเงินอิเล็กทรอนิกส์ (e-money) และบัตรเครดิตที่ให้บริการในวงกว้างและมีปริมาณธุรกรรมอย่างมีนัยสำคัญ และ (3) ผู้ให้บริการสินเชื่อภายใต้การกำกับของ ธปท. ทุกราย เนื่องจากลูกค้ารายย่อยและ SMEs ใช้บริการสินเชื่อกระจายตัวกับผู้ให้บริการทั้งรายใหญ่และรายเล็ก โดย ธปท. จะหารือกับผู้ที่เกี่ยวข้องถึงแนวทางช่วยลดภาระการจัดทำกลไกให้แก่ผู้ให้บริการรายเล็กต่อไป

2.2 ขอบเขตของผู้ให้บริการที่สามารถรับข้อมูลของลูกค้า (ผู้ให้บริการที่รับข้อมูล) ต้องครอบคลุมผู้ให้บริการที่สามารถนำข้อมูลของลูกค้าไปใช้เพื่อประโยชน์ในการพัฒนาและนำเสนอบริการที่ตอบโจทย์ลูกค้าได้ดีขึ้น และได้รับการกำกับดูแลอย่างเหมาะสมและได้มาตรฐาน เพื่อให้มั่นใจว่าการรับส่งข้อมูลของลูกค้ามีความปลอดภัยและมีการดูแลลูกค้าอย่างเหมาะสม ซึ่งได้แก่ **(1) ผู้ให้บริการทางการเงินภายใต้การกำกับของ ธปท.** ประกอบด้วย สถาบันการเงิน และ SFIs ตาม พ.ร.บ. ธุรกิจสถาบันการเงิน ผู้ให้บริการการชำระเงิน และผู้ให้บริการสินเชื่อภายใต้การกำกับของ ธปท. และ **(2) ผู้ให้บริการอื่น ๆ ที่ได้รับการกำกับดูแลภายใต้หลักเกณฑ์ที่มีมาตรฐานในระดับเดียวกัน** โดยในระยะแรกจะมุ่งเน้นที่ผู้ให้บริการทางการเงินภายใต้

การกำกับของสำนักงาน ก.ล.ต. และสำนักงาน คปภ. ทั้งนี้ ในอนาคตสามารถขยายขอบเขตไปยังผู้ให้บริการในภาคส่วนอื่นที่ได้รับการกำกับภายใต้หลักเกณฑ์ที่มีมาตรฐานในระดับเดียวกันได้

2.3 หลักการในการกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล จะต้องพิจารณาถึงการส่งเสริมการใช้สิทธิของลูกค้า ในขณะเดียวกันไม่ทำให้เกิดการรับส่งข้อมูลเกินความจำเป็น โดย (1) ผู้ให้บริการต้องไม่กำหนดเงื่อนไขหรือมีการดำเนินการที่เป็นอุปสรรคต่อการรับส่งหรือต่อการใช้ประโยชน์จากข้อมูล และ (2) ผู้ให้บริการต้องไม่คิดค่าธรรมเนียมที่เกี่ยวข้องกับการใช้สิทธิรับส่งข้อมูลของลูกค้าตามเกณฑ์นี้ เว้นแต่ในกรณีที่มีการเรียกข้อมูลสูงเกินกว่าระดับปกติที่กำหนด (threshold) ที่ผู้ให้บริการอาจคิดค่าธรรมเนียมเพื่อไม่ให้มีการเรียกข้อมูลเกินความจำเป็น

2.4 การกำกับดูแลด้านการคุ้มครองผู้บริโภค และการรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและปลอดภัย โดย ธปท. กำหนดแนวทางกำกับดูแลผู้ให้บริการในเรื่องดังกล่าวเพื่อให้ลูกค้ามีความมั่นใจในการใช้สิทธิส่งข้อมูลทั้งก่อน ระหว่าง และหลังจากการใช้สิทธิ แต่ไม่ก่อให้เกิดภาระต่อผู้ให้บริการมากจนเกินไปและไม่กลายเป็นเงื่อนไขที่จะเป็นอุปสรรคต่อการรับส่งข้อมูล ดังนี้ **(1) การคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูล (data privacy)** โดยผู้ให้บริการต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูลที่บังคับใช้ในปัจจุบัน เช่น PDPA และถือปฏิบัติตามหลักเกณฑ์ที่ ธปท. กำหนดเพิ่มเติมในเรื่องการขอความยินยอม (consent) และกระบวนการยืนยันตัวตน (authentication) และการให้ลูกค้ายืนยันการใช้สิทธิ (authorization) ก่อนการส่งข้อมูลที่ได้มาตรฐาน โดยต้องแยกข้อความและแจ้งข้อมูลและเงื่อนไขการให้บริการแก่ลูกค้าอย่างเพียงพอและชัดเจน รวมทั้งต้องให้ลูกค้าสามารถบริหารจัดการและตรวจสอบ consent และ authorization ที่เคยให้ไว้ได้โดยง่ายและสะดวก **(2) การรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและการบริหารจัดการข้อมูลให้มีความปลอดภัย** โดยผู้ให้บริการต้องปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติที่ ธปท. กำหนด รวมทั้งต้องมีการบริหารจัดการข้อมูลที่ดีเพื่อให้มั่นใจว่าข้อมูลที่ผู้ให้บริการรับส่งและขั้นตอนที่เกี่ยวข้องได้รับการดูแลด้านความปลอดภัยและความเป็นส่วนบุคคลของข้อมูลตลอดกระบวนการ ซึ่งครอบคลุมทั้งการกำกับดูแลกิจการให้มีธรรมาภิบาลในการบริหารจัดการข้อมูล โดยเฉพาะคณะกรรมการและผู้บริหารระดับสูงที่ต้องให้ความสำคัญในเรื่องนี้ การรักษาความมั่นคงปลอดภัยของข้อมูล และการบริหารจัดการเมื่อเกิดเหตุผิดปกติหรือปัญหาเกี่ยวกับข้อมูล

2.5 กระบวนการกำกับดูแลผู้ให้บริการให้ได้มาตรฐาน ธปท. มีกระบวนการกำกับดูแลผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลของลูกค้าให้ปฏิบัติตามหลักเกณฑ์ฉบับนี้อย่างต่อเนื่อง ดังนี้ (1) **ก่อนเริ่มให้บริการรับส่งข้อมูลของลูกค้า** ผู้ให้บริการต้องผ่านการทดสอบการปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติที่กำหนด **(2) ระหว่างการให้บริการ** ธปท. จะมีการติดตามและกำกับดูแลผู้ให้บริการอย่างต่อเนื่อง โดยหากพบว่าระบบหรือการให้บริการตามหลักเกณฑ์ฉบับนี้มีปัญหาหรือข้อบกพร่อง ธปท. สามารถสั่งการให้ผู้ให้บริการดำเนินการแก้ไขได้ และ **(3) เมื่อเกิดปัญหาหรือข้อพิพาทกับลูกค้า** ผู้ให้บริการต้องรายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญให้ ธปท. ทราบโดยเร็ว และในกรณีที่ผู้ให้บริการเป็นผู้กระทำผิดหรือเป็น

ผู้รับผิดชอบปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว ต้องมีการดูแล แก้ไข เยียวยาแก่ลูกค้าอย่างเหมาะสม รวมถึงมีแนวทางป้องกันปัญหามิให้เกิดขึ้นซ้ำอีก

2.6 กำหนดการดำเนินการตามหลักเกณฑ์ ธปท. กำหนดให้ผู้ให้บริการต้องทำกลไกให้แล้วเสร็จพร้อมให้ลูกค้าใช้สิทธิส่งข้อมูลได้ โดยเริ่มจากข้อมูลเงินฝาก ที่สามารถพัฒนาต่อยอดจากมาตรฐานที่มีอยู่ในปัจจุบัน ตามมาด้วยข้อมูลสินเชื่อและการชำระเงิน และเริ่มจากข้อมูลลูกค้าประเภทบุคคลธรรมดา ตามมาด้วยข้อมูลลูกค้าประเภทนิติบุคคล เพื่อให้เวลาในการพัฒนาระบบสำหรับการส่งข้อมูลนิติบุคคล โดยมีกำหนดการดังนี้ **(1) ข้อมูลเงินฝากของบุคคลธรรมดา และข้อมูลสินเชื่อและการชำระเงินของบุคคลธรรมดา** เริ่มให้บริการได้ภายใน 6 ไตรมาส และ 7 ไตรมาส นับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 4 ปี 2569 และไตรมาสที่ 1 ปี 2570) ตามลำดับ และ (**2) ข้อมูลเงินฝากของนิติบุคคล และข้อมูลสินเชื่อและการชำระเงินของนิติบุคคล** เริ่มให้บริการได้ภายใน 9 ไตรมาส และ 10 ไตรมาส นับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 3 และ ไตรมาสที่ 4 ปี 2570) ตามลำดับ เว้นแต่กรณีมีเหตุจำเป็นอันสมควรจากปัจจัยที่ผู้ให้บริการไม่สามารถควบคุมได้ ให้ผู้ให้บริการยื่นขอผ่อนผันต่อ ธปท. เป็นรายกรณี โดยแสดงเหตุผลความจำเป็น และรายละเอียดที่เกี่ยวข้อง

1. บทนำ

การเปิดกว้างให้มีการใช้ประโยชน์จากข้อมูล (open data) เป็นหนึ่งในแนวนโยบายสำคัญภายใต้ภูมิทัศน์ใหม่ภาคการเงินไทยด้านการเงินดิจิทัล[1] ที่จะทำให้ภาคการเงินสามารถใช้ประโยชน์จากเทคโนโลยีและข้อมูลในการพัฒนานวัตกรรมและบริการทางการเงินเพื่อตอบโจทย์ลูกค้าแต่ละกลุ่มได้ดีขึ้นด้วยต้นทุนที่ต่ำลง และมีความรับผิดชอบต่อสังคม (responsible innovation)

ในการพัฒนาระบบการเงินดิจิทัล นอกจากการนำระบบการชำระเงินความเร็วสูง (fast payment) หรือ PromptPay มาใช้ในประเทศไทยจะเป็นจุดเปลี่ยนที่สำคัญ (game changer) ซึ่งช่วยให้การชำระเงินทำได้เร็วและสะดวกขึ้นแล้ว การทำให้ข้อมูลที่เก็บอยู่ตามที่ต่าง ๆ ไหลเวียนและนำไปใช้ประโยชน์ได้อย่างเต็มศักยภาพมากขึ้น จะเป็นอีกหนึ่งจุดเปลี่ยนที่สำคัญที่จะนำไปสู่การพัฒนานวัตกรรมทางการเงินดิจิทัล ซึ่งจะช่วยยกระดับบริการให้มีประสิทธิภาพและตอบโจทย์ความต้องการของผู้ใช้บริการได้ดีขึ้น โดยเฉพาะ **(1) การเข้าถึงสินเชื่อในระบบอย่างเหมาะสม** โดยเฉพาะรายย่อยที่ไม่มีรายได้ประจำและผู้ประกอบการรายเล็กที่มีข้อมูลประวัติทางการเงินกับสถาบันการเงินไม่มากพอ แต่มีความสามารถและมีข้อมูลอื่นอยู่ตามที่ต่าง ๆ และ **(2) การบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล** โดยเฉพาะลูกค้ารายย่อยและผู้ประกอบการรายเล็ก โดยสามารถรวมข้อมูลบัญชีทางการเงินไว้ที่เดียวเพื่อต่อยอดไปยังบริการอื่น ๆ ที่เหมาะกับวิถีชีวิตของแต่ละบุคคลมากขึ้น ซึ่งยังเป็นช่องว่างสำคัญในระบบการเงินไทย

อย่างไรก็ดี ในปัจจุบันข้อมูลของลูกค้ายังกระจัดกระจายอยู่กับผู้ให้บริการและหน่วยงานต่าง ๆ ซึ่งหากมีกลไกที่ลูกค้าสามารถขอให้ผู้ให้บริการหรือหน่วยงานที่เก็บข้อมูลส่งข้อมูลของตนไปยังหน่วยงานอื่น

[1] ศึกษารายละเอียดเพิ่มเติมของแนวนโยบายสำคัญภายใต้ภูมิทัศน์ใหม่ภาคการเงินไทยในด้านการเงินดิจิทัล ได้ที่ https://www.bot.or.th/content/dam/bot/financial-innovation/financial-landscape/ConsultationPaper-FinancialLandscape-TH.pdf

ได้สะดวก ตามสิทธิภายใต้กฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) จะช่วยให้ลูกค้าสามารถใช้ประโยชน์จากข้อมูลเหล่านั้น เพื่อให้ได้รับบริการทางการเงินที่ดีขึ้นได้

หลายประเทศ เช่น สิงคโปร์ สหราชอาณาจักร ออสเตรเลีย เกาหลีใต้ อินเดีย บราซิล **ได้พัฒนากลไกให้ประชาชนสามารถใช้สิทธิตามกฎหมายส่งข้อมูลของตนที่มีอยู่กับผู้ให้บริการและหน่วยงานต่าง ๆ ได้ โดยส่วนใหญ่เริ่มจากข้อมูลภาคสถาบันการเงิน** เช่น ข้อมูลบัญชีเงินฝาก ข้อมูลการชำระเงิน ซึ่งเป็นข้อมูลพื้นฐานสำคัญที่ผู้ให้บริการทางการเงินส่วนใหญ่ใช้พิจารณาสินเชื่อและนำเสนอบริการใหม่ ๆ ที่ตอบโจทย์ลูกค้าได้ดีขึ้น เช่น

- **ประชาชนและผู้ประกอบการ** สามารถบริหารจัดการบัญชีทางการเงินผ่านแอปพลิเคชันเดียวบนมือถือแบบรวมศูนย์ได้ (consolidated account information) โดยสามารถเรียกดูข้อมูลบัญชีของตนที่อยู่กับผู้ให้บริการต่าง ๆ และส่งข้อมูลดังกล่าวให้ผู้ให้บริการรายอื่นได้สะดวก
- **ผู้ให้บริการ** สามารถเข้าถึงและใช้ข้อมูลของลูกค้าในรูปแบบดิจิทัลจากแหล่งข้อมูลต้นทางหลายแหล่งได้ เช่น ข้อมูลการเดินบัญชีของลูกค้าที่มีกับหลายสถาบันการเงิน ซึ่งสามารถนำไปประมวลผลต่อได้สะดวก ทำให้ลดขั้นตอนและต้นทุนการให้บริการ
- **มีบริการใหม่ ๆ ที่ต่อยอดจากการนำข้อมูลที่รวบรวมได้ไปใช้ประโยชน์** เช่น ในสหราชอาณาจักรและเกาหลีใต้มีผู้ให้บริการรวบรวมข้อมูลของลูกค้ามาประมวลและคำนวณคะแนนเครดิตเบื้องต้น รวมถึงส่งข้อมูลเหล่านี้ให้แก่ผู้ให้บริการสินเชื่อหลายรายภายใต้ความยินยอม (consent) ของลูกค้า ช่วยเพิ่มทางเลือกและโอกาสในการเข้าถึงสินเชื่อในระบบแก่ลูกค้า และในสิงคโปร์มีการนำข้อมูลที่รวบรวมได้มาวิเคราะห์และนำเสนอบริการต่อยอดด้านการออม การลงทุน และประกันชีวิตที่เหมาะกับวิถีชีวิตของแต่ละบุคคล

ในกรณีของไทย ธนาคารแห่งประเทศไทย (ธปท.) คาดหวังว่า เมื่อข้อมูลของลูกค้าสามารถไหลเวียนได้สะดวกและผู้ให้บริการสามารถนำข้อมูลเหล่านี้มาใช้ประโยชน์ในการทำความรู้จักและเข้าใจลูกค้าได้มากขึ้น ผู้ให้บริการก็จะสามารถออกแบบและนำเสนอบริการทางการเงินที่เหมาะและตอบโจทย์ลูกค้าแต่ละคนได้ดีขึ้น เช่น ในกรณีลูกค้าต้องการเงินทุน ก็สามารถนำเสนอสินเชื่อที่มีวงเงิน อัตราดอกเบี้ย และระยะเวลาชำระคืนที่เหมาะสมกับความสามารถและรายรับรายจ่ายของลูกค้า ในกรณีที่ลูกค้ามีเงินเหลือ ก็สามารถแนะนำให้ลูกค้านำเงินดังกล่าวไปลงทุนเพื่อหาผลตอบแทนที่ดีขึ้นและเหมาะกับระดับความเสี่ยงที่ลูกค้ารับได้ เป็นต้น

ทั้งนี้ ภาครัฐหรือธนาคารกลางในหลายประเทศได้ออกกฎหมายหรือกฎเกณฑ์ เพื่อผลักดันให้เกิดกลไกที่ประชาชนสามารถใช้สิทธิส่งข้อมูลระหว่างหน่วยงานต่าง ๆ ได้สะดวกและปลอดภัย รวมทั้งให้ภาคส่วนที่เกี่ยวข้องมีส่วนร่วมในการออกแบบและพัฒนามาตรฐานกลาง และแนวปฏิบัติสำหรับการเชื่อมต่อและรับส่งข้อมูลผ่านกลไกดังกล่าว เพื่อให้มีมาตรฐานเดียวกัน อันจะช่วยสร้างความมั่นใจเรื่องความปลอดภัย และช่วยลดต้นทุนและความซ้ำซ้อนในการพัฒนามาตรฐาน

สำหรับประเทศไทย **ธปท. หน่วยงานภาครัฐ หน่วยงานกำกับดูแลภาคการเงินอื่น ๆ และผู้ให้บริการทางการเงินที่เกี่ยวข้อง**[2] **ได้ร่วมกันผลักดันโครงการ "Your Data ข้อมูลของคุณ สู่บริการทางการเงินที่ตอบโจทย์"** เพื่อให้มีกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนทั้งในภาคการเงินและนอกภาคการเงินผ่านช่องทางดิจิทัลได้สะดวก ปลอดภัย ไม่ถูกปิดกั้น และใช้งานได้จริง เพื่อให้สามารถเข้าถึงและได้รับบริการทางการเงินที่ดีขึ้น โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล โดยมีข้อมูลชุดแรกที่จะผลักดันให้มีกลไกดังกล่าว ดังนี้

1) ข้อมูลในภาคการเงิน ซึ่งแสดงให้เห็นถึงรายรับรายจ่าย พฤติกรรมการใช้จ่ายเงิน และพฤติกรรมการชำระหนี้ รวมทั้งการถือครองสินทรัพย์ทางการเงิน โดยในส่วนของข้อมูลที่อยู่กับผู้ให้บริการภายใต้การกำกับของ ธปท. ได้แก่ **ข้อมูลบัญชีเงินฝาก ข้อมูลการชำระเงิน (e-money และบัตรเครดิต) และข้อมูลสินเชื่อ** ธปท. จะผลักดันให้ผู้ให้บริการภายใต้การกำกับของ ธปท. จัดทำข้อมูลและกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลดังกล่าวได้ สำหรับ**ข้อมูลการถือครองหลักทรัพย์และกรมธรรม์ประกันภัย** ธปท. จะร่วมกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ผลักดันให้มีการพัฒนากลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลระหว่างผู้ให้บริการในภาคการเงินได้ต่อไป

2) ข้อมูลนอกภาคการเงิน ซึ่งแสดงให้เห็นถึงรายรับรายจ่าย พฤติกรรมการใช้จ่ายอื่น ๆ โดย ธปท. อยู่ระหว่างดำเนินการร่วมกับสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หน่วยงานสาธารณูปโภคที่เกี่ยวข้อง และกรมสรรพากร ในการพัฒนาช่องทางให้ประชาชนสามารถส่ง**ข้อมูลการใช้และการจ่ายชำระค่าไฟฟ้าและน้ำประปา และข้อมูลแบบภาษี**ให้กับผู้ให้บริการทางการเงินได้ โดยคาดว่าลูกค้าจะเริ่มส่งได้ภายในปี 2568

ทั้งนี้ การผลักดันให้เกิดกลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่กับผู้ให้บริการทางการเงินภายใต้การกำกับของ ธปท. ได้นั้น จำเป็นต้องอาศัยทั้ง (1) การวางกฎกติกา โดย ธปท. จะออกเกณฑ์กำหนดให้ผู้ให้บริการภายใต้กำกับของ ธปท. ที่เก็บข้อมูลของลูกค้าจัดทำข้อมูลและกลไกรับส่งข้อมูลในรูปแบบที่พร้อมให้ลูกค้าใช้สิทธิโดยสะดวก ปลอดภัย และไม่ถูกปิดกั้น **และ (2) การมีส่วนร่วมจากผู้ที่เกี่ยวข้อง** โดย ธปท. จะร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำมาตรฐานกลางและแนวปฏิบัติที่จะใช้ร่วมกันในการรับส่งข้อมูล[3]

---

[2] กระทรวงการคลัง สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) กรมสรรพากร สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) การไฟฟ้านครหลวง การไฟฟ้าส่วนภูมิภาค การประปานครหลวง การประปาส่วนภูมิภาค และสมาคมผู้ให้บริการทางการเงินที่เกี่ยวข้อง ได้แก่ สมาคมธนาคารไทย สมาคมสถาบันการเงินของรัฐ สมาคมธนาคารนานาชาติ ชมรมสินเชื่อส่วนบุคคล สมาคมการค้าผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ไทย สมาคมฟินเทคประเทศไทย สมาคมบริษัทหลักทรัพย์ไทย สมาคมบริษัทจัดการลงทุน สมาคมประกันวินาศภัยไทย สมาคมประกันชีวิตไทย

[3] ซึ่งจะครอบคลุมถึงมาตรฐานการรับส่งและดูแลความปลอดภัยของข้อมูล (data & IT security) มาตรฐานการเชื่อมต่อโปรแกรม (Application Programming Interface standard: API standard) รวมถึงกำหนดแนวปฏิบัติและกระบวนการที่เกี่ยวข้อง เช่น การเก็บและการรับส่งข้อมูลเพื่อให้เป็นไปตามหลักธรรมาภิบาลในการบริหารจัดการข้อมูลและมีการดูแลความเป็นส่วนบุคคลของข้อมูล (data governance & data privacy) การออกแบบการใช้งานที่สะดวกและสร้างประสบการณ์ที่ดีแก่ลูกค้า (customer experience) การดูแลแก้ไขเมื่อเกิดปัญหา

เพื่อให้มั่นใจว่าใช้งานได้จริง **โดยจะดำเนินการร่วมกันผ่านคณะกรรมการขับเคลื่อนและคณะทำงาน**[4] ซึ่งประกอบด้วยผู้แทนจากสมาคมผู้ให้บริการต่าง ๆ ได้แก่ ธนาคารพาณิชย์ (ธพ.) สถาบันการเงินเฉพาะกิจ (SFIs) ผู้ให้บริการสินเชื่อ ผู้ให้บริการการชำระเงิน ผู้ให้บริการเทคโนโลยีทางการเงิน (financial technology หรือฟินเทค) หน่วยงานที่พัฒนามาตรฐานและหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงมีผู้แทนจากสมาคมผู้บริโภคและ SMEs เป็นคณะที่ปรึกษา

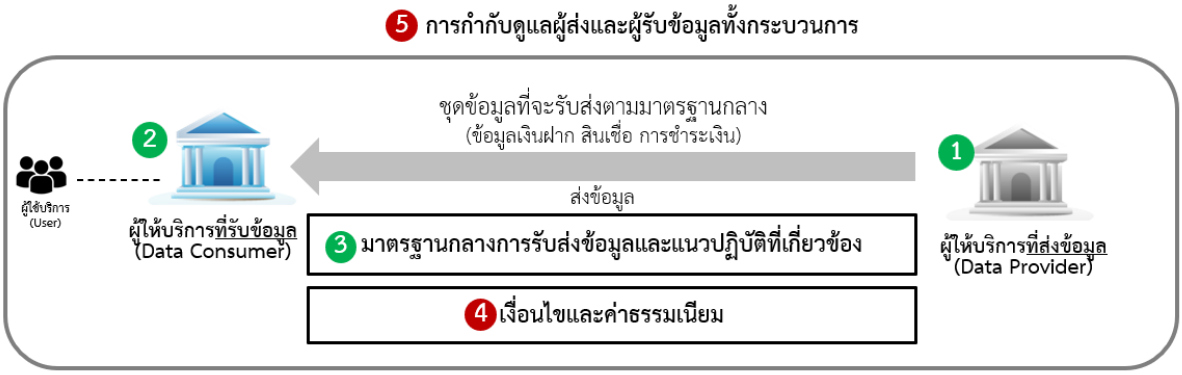
เอกสารฉบับนี้มีวัตถุประสงค์เพื่อรับความเห็นต่อแนวทางการกำกับดูแลให้ผู้ให้บริการจัดทำกลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่กับภาคสถาบันการเงินได้ (ร่างหลักเกณฑ์ฯ) เพื่อประโยชน์ในการได้รับบริการทางการเงินที่ตอบโจทย์ได้ดีขึ้น โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล โดยในระยะแรกจะเน้นให้ผู้ให้บริการที่เป็นผู้รับข้อมูลให้สามารถนำข้อมูลที่ได้รับจากลูกค้าไปใช้ประโยชน์ในการพัฒนาและนำเสนอบริการทางการเงินของผู้ให้บริการรายนั้น ๆ ให้สามารถตอบโจทย์ลูกค้าได้ดีขึ้นก่อน และในระยะต่อไป ธปท. จะพิจารณาแนวทางการอนุญาตและกำกับดูแลผู้ให้บริการที่รวบรวมและบริหารจัดการข้อมูลภายใต้ consent ของลูกค้าในฐานะบุคคลที่สาม (Third Party Data Aggregator) ซึ่งทำหน้าที่รวบรวมข้อมูลของลูกค้าจากที่ต่าง ๆ มาแสดงผลและให้ลูกค้าสามารถบริหารจัดการได้ในที่เดียว รวมถึงช่วยวิเคราะห์หรือประมวลผลในเบื้องต้น เช่น การคำนวณคะแนนเครดิต (credit scoring) ในเบื้องต้น รวมทั้งให้บริการส่งข้อมูลของลูกค้าไปยังผู้ให้บริการหรือหน่วยงานอื่น ๆ

[4] คณะกรรมการขับเคลื่อนและคณะทำงานประกอบด้วยผู้แทนจาก ธปท. สมาคมธนาคารไทย สมาคมสถาบันการเงินของรัฐ สมาคมธนาคารนานาชาติ ชมรมสินเชื่อส่วนบุคคล สมาคมการค้าผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ไทย สมาคมฟินเทคแห่งประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และผู้ทรงคุณวุฒิ นอกจากนี้ มีหน่วยงานกำกับดูแลร่วมให้คำแนะนำและเชื่อมโยงนโยบายที่อาจต่อยอดไปยังภาคส่วนอื่น รวมถึงผู้แทนจากสมาคมผู้บริโภคและ SME ให้ความเห็นต่อรูปแบบบริการที่ตอบโจทย์ความต้องการ

2. หลักการสำคัญ

ประชาชนซึ่งเป็นเจ้าของข้อมูลมีสิทธิขอให้ผู้ที่เก็บรวบรวมข้อมูลของตนส่งข้อมูลไปยังหน่วยงานอื่นได้ด้วยวิธีการอัตโนมัติ หากผู้ที่เก็บรวบรวมข้อมูลได้จัดทำข้อมูลนั้นให้อยู่ในรูปแบบที่พร้อมนำไปประมวลผลต่อ และมีระบบรับส่งข้อมูลด้วยวิธีอัตโนมัติไว้รองรับการใช้สิทธิของเจ้าของข้อมูลตามมาตรา 31 แห่ง PDPA

ธปท. จึงกำหนดให้ผู้ให้บริการภายใต้การกำกับของ ธปท. จัดทำกลไกให้ลูกค้าที่เป็นเจ้าของข้อมูลสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่กับผู้ให้บริการได้อย่างสะดวก ปลอดภัย ไม่ถูกปิดกั้น โดยมีหลักการดังต่อไปนี้



สิ่งที่อยากเห็น (Green Line (GL))

1) ผู้ให้บริการที่ส่งข้อมูล (Data Provider) ได้แก่ ผู้ให้บริการทางการเงินที่เก็บข้อมูลที่มีนัยสำคัญต่อลูกค้า ต้องจัดทำข้อมูลและกลไกที่พร้อมให้ลูกค้าใช้สิทธิส่งข้อมูลผ่านช่องทางดิจิทัลได้สะดวก (GL1)

2) ผู้ให้บริการที่รับข้อมูล (Data Consumer) ได้แก่ ผู้ให้บริการสามารถได้รับข้อมูลของลูกค้าและนำข้อมูลดังกล่าวไปใช้พัฒนาและนำเสนอบริการทางการเงินที่ตอบโจทย์ โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล ซึ่งรวมถึง Third Party Data Aggregator ซึ่ง ธปท. จะพิจารณาออกหลักเกณฑ์เพิ่มเติมในระยะถัดไป (GL2)

3) การเชื่อมต่อและรับส่งข้อมูล ระหว่างผู้ให้บริการที่รับและส่งข้อมูลต้องเป็นไปตามมาตรฐานกลางและแนวปฏิบัติที่กำหนด เพื่อให้มีประสิทธิภาพและไม่เกิดภาระหรือต้นทุนเกินความจำเป็น (GL3)

สิ่งที่ไม่อยากเห็น (Red Line (RL))

1) เงื่อนไขและค่าธรรมเนียม เป็นอุปสรรคต่อการใช้งานและการรับส่งข้อมูล (RL1.1) หรือเกิดการเรียกข้อมูลเกินความจำเป็น รวมถึงเกิดการรับข้อมูลเพียงอย่างเดียวโดยไม่ส่งข้อมูลให้ผู้ให้บริการรายอื่น (RL1.2)

2) ผู้ให้บริการดูแลความเสี่ยงไม่เหมาะสม โดยเฉพาะด้านการรักษาความปลอดภัยข้อมูล (data security) ความเป็นส่วนบุคคลของข้อมูล (data privacy) และการคุ้มครองผู้บริโภค (consumer protection) (RL2)

3. สาระสำคัญของแนวทางการกำกับดูแลให้มีกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่กับภาคสถาบันการเงินได้[5]

3.1 ขอบเขตผู้ให้บริการภายใต้การกำกับของ ธปท. ที่ต้องทำกลไกให้พร้อมส่งข้อมูลของลูกค้าทางดิจิทัลเมื่อลูกค้าร้องขอ (ผู้ให้บริการที่ส่งข้อมูล หรือ Data Provider)

หลักการ: *การกำหนดให้ผู้ให้บริการต้องทำกลไกที่พร้อมให้ลูกค้าใช้สิทธิส่งข้อมูลผ่านช่องทางดิจิทัลได้สะดวกต้อง (1) ครอบคลุมผู้ให้บริการทางการเงินที่เก็บข้อมูลที่มีนัยสำคัญต่อลูกค้า เพื่อให้สามารถนำข้อมูลไปใช้ประโยชน์ได้จริง โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล (GL1) และ (2) ไม่เป็นภาระหรือต้นทุนเกินความจำเป็นต่อผู้ให้บริการ (GL3)*[6]

ธปท. จะกำหนดให้ผู้ให้บริการทางการเงินภายใต้การกำกับดูแลของ ธปท. ที่มีข้อมูลบัญชีเงินฝาก ข้อมูลการชำระเงินผ่าน e-money และบัตรเครดิต และข้อมูลสินเชื่อ[7] ที่มีนัยสำคัญต่อลูกค้า ดังต่อไปนี้ ต้องจัดทำกลไกพร้อมส่งข้อมูลของลูกค้าผ่านช่องทางดิจิทัลได้สะดวก เมื่อลูกค้าใช้สิทธิ

1) สถาบันการเงิน และ SFIs ตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ที่ให้บริการเงินฝากแก่ลูกค้าอย่างมีนัยสำคัญ โดยเป็นผู้ให้บริการที่มีจำนวนบัญชีเงินฝากตั้งแต่ 100,000 บัญชีขึ้นไป[8] ต้องจัดทำกลไกส่งข้อมูล[9]

2) ผู้ให้บริการการชำระเงินในวงกว้างที่มีปริมาณธุรกรรมอย่างมีนัยสำคัญ ซึ่งได้แก่ ผู้ให้บริการ e-money ที่ให้บริการชำระเงินนอกกลุ่มธุรกิจตนเองได้[10] และผู้ให้บริการบัตรเครดิต โดยเป็นผู้ให้บริการที่มีปริมาณธุรกรรมตั้งแต่ 1 ล้านครั้งต่อปี[11] ต้องจัดทำกลไกส่งข้อมูล[12]

---

[5] โดยอาศัยอำนาจตามกฎหมายที่ใช้ในการกำกับดูแลผู้ให้บริการแต่ละประเภท ได้แก่ (1) พระราชบัญญัติ ธุรกิจสถาบันการเงิน พ.ศ. 2551 สำหรับ ธพ. SFIs บริษัทเงินทุน (บง.) และบริษัทเครดิตฟองซิเอร์ (บค.) (2) ประกาศของคณะปฏิวัติ ฉบับที่ 58 (ปว. 58) และประกาศกระทรวงการคลังที่ออกโดยอาศัยอำนาจตาม ปว. 58 กรณีผู้ประกอบธุรกิจตาม ปว. 58 ที่อยู่ภายใต้การกำกับของ ธปท. และ (3) พ.ร.บ. ระบบการชำระเงิน พ.ศ. 2560 สำหรับผู้ประกอบธุรกิจบริการการชำระเงิน

[6] ประเทศบราซิล และสหราชอาณาจักร ใช้ปัจจัยนี้ในการกำหนดขอบเขตผู้ให้บริการที่ต้องจัดทำกลไกดังกล่าว

[7] ได้แก่ ธพ. บง. บค. SFIs ผู้ให้บริการสินเชื่อส่วนบุคคลภายใต้การกำกับ (personal loan) ผู้ให้บริการสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ (nano finance) ผู้ให้บริการบัตรเครดิต ผู้ให้บริการเงินอิเล็กทรอนิกส์ (e-money) และผู้ให้บริการธุรกิจระบบเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล (peer-to-peer lending platform)

[8] มีจำนวนบัญชีเงินฝาก ตั้งแต่ 100,000 บัญชี ขึ้นไป โดยคำนวณจากค่าเฉลี่ยจำนวนบัญชีเงินฝาก ณ สิ้นเดือน 12 เดือน (12-month average) นับย้อนขึ้นไปจากเดือนที่หลักเกณฑ์มีผลบังคับใช้ ทั้งนี้ ให้ถือปฏิบัติตามเกณฑ์ไปตลอด แม้ว่าต่อมาจะมียอดที่คำนวณได้ลดลงต่ำกว่า threshold ที่กำหนด

[9] จากข้อมูลปี 2566 ผู้ให้บริการที่เข้าข่ายข้างต้นครอบคลุมจำนวนบัญชีเงินฝากคิดเป็นร้อยละ 99.95 ของจำนวนบัญชีเงินฝากทั้งหมด

[10] หมายถึง ผู้ให้บริการ e-money ซึ่งต้องขออนุญาตประกอบธุรกิจ ตามข้อ 2 ในส่วนข้อ 2.2 ของประกาศกระทรวงการคลัง เรื่อง การกำหนดบริการการชำระเงินภายใต้การกำกับ อย่างไรก็ดี อาจมีผู้ให้บริการ e-money บางรายที่ได้รับอนุญาตตามข้อ 2 ในส่วนข้อ 2.2 แต่ให้บริการในบางผลิตภัณฑ์ในวงจำกัดตาม ข้อ 2.2.1 – 2.2.4 เช่น ผู้ให้บริการ e-money ที่รับทำ e-money ให้บริษัทต่าง ๆ ที่เป็นผู้ว่าจ้างหรือเป็นพันธมิตรทางธุรกิจ เพื่อใช้ในธุรกิจของบริษัทที่เป็นลูกค้าเหล่านั้น ธปท. จึงจะกำหนดให้ผู้ให้บริการ e-money เหล่านี้ สามารถยื่นขอยกเว้นการส่งข้อมูลธุรกรรมของผลิตภัณฑ์ที่ให้บริการในวงจำกัดเป็นรายผลิตภัณฑ์ ให้ ธปท. พิจารณาได้เป็นรายกรณี

[11] หมายถึง ธุรกรรมทั้งหมดของผู้ให้บริการ ซึ่งรวมถึงการชำระค่าสินค้าและค่าบริการ การชำระค่าสาธารณูปโภค การเติมเงิน การถอนเงิน และการโอนเงิน โดยมีปริมาณธุรกรรมทั้งปีตั้งแต่ 1 ล้านครั้งขึ้นไป ซึ่งคำนวณจากผลรวมปริมาณธุรกรรม 12 เดือน จาก 14 เดือนล่าสุดนับย้อนขึ้นไปจากเดือนที่หลักเกณฑ์มีผลบังคับใช้ โดยไม่นับรวมเดือนที่มีปริมาณธุรกรรมมากที่สุดและเดือนที่มีปริมาณธุรกรรมน้อยที่สุด ทั้งนี้ ให้ถือปฏิบัติตามเกณฑ์ไปตลอด แม้ว่าต่อไปจะมียอดปริมาณธุรกรรมรวมต่ำกว่า threshold ที่กำหนด

[12] จากข้อมูลปี 2566 ผู้ให้บริการที่เข้าข่ายข้างต้นครอบคลุมผู้ให้บริการที่มีธุรกรรมรวมกันคิดเป็นร้อยละ 99.9 ของปริมาณธุรกรรมทั้งหมด

3) ผู้ให้บริการสินเชื่อภายใต้การกำกับของ ธปท.[13] ทุกราย เนื่องจากลูกค้ารายย่อยและ SMEs ใช้บริการสินเชื่อกระจายตัวทั้งกับผู้ให้บริการทั้งรายใหญ่และรายเล็ก โดย

3.1) ผู้ให้บริการสินเชื่อที่มีจำนวนบัญชีสินเชื่อตั้งแต่ 100,000 บัญชี <u>หรือ</u>ยอดสินเชื่อคงค้างตั้งแต่ 1,000 ล้านบาท[14] ต้องจัดให้มีกลไกให้ลูกค้าใช้สิทธิส่งข้อมูลหรือนำข้อมูลของตนมาใช้ประโยชน์ได้ด้วยวิธีใดวิธีหนึ่งระหว่าง (1) การเข้าเป็นสมาชิกบริษัทข้อมูลเครดิต <u>หรือ</u> (2) การจัดทำกลไกส่งข้อมูลตามหลักเกณฑ์ฉบับนี้

3.2) ผู้ให้บริการสินเชื่อที่มีจำนวนบัญชีสินเชื่อน้อยกว่า 100,000 บัญชี <u>และ</u>ยอดสินเชื่อคงค้างน้อยกว่า 1,000 ล้านบาท นอกจากทางเลือกตามข้อ 3.1) แล้ว ผู้ให้บริการอาจเลือกจัดทำช่องทางให้ลูกค้าสามารถเรียกข้อมูลของตนที่อยู่ในรูปแบบ machine readable เพื่อให้ลูกค้านำไปใช้ประโยชน์ หรือส่งให้ผู้ให้บริการรายอื่นด้วยตนเองก็ได้ ทั้งนี้ ธปท. จะหารือกับผู้ที่เกี่ยวข้องถึงแนวทางช่วยลดภาระการจัดทำกลไกแก่ผู้ให้บริการรายเล็กในรายละเอียดต่อไป

อนึ่ง ผู้ให้บริการเงินฝากและผู้ให้บริการการชำระเงินที่ไม่เข้าข่ายตามขอบเขตที่กำหนดให้ต้องจัดทำกลไกข้างต้น[15] แต่ประสงค์ที่จะรับข้อมูลของลูกค้าภายใต้หลักเกณฑ์ฉบับนี้สามารถเข้าร่วมจัดทำกลไกได้ตามความสมัครใจและตามความพร้อม โดยต้องทำหน้าที่เป็นผู้ส่งข้อมูลด้วยตามหลักต่างตอบแทน (reciprocity) และปฏิบัติตามเกณฑ์ มาตรฐานกลาง และแนวปฏิบัติที่เกี่ยวข้อง

3.2 ขอบเขตของผู้ให้บริการที่สามารถรับข้อมูลของลูกค้า (ผู้ให้บริการที่รับข้อมูล หรือ Data Consumer)

หลักการ: *การพิจารณาผู้ให้บริการที่สามารถรับข้อมูลของลูกค้าได้ต้อง*
(1) ครอบคลุมผู้ให้บริการที่สามารถนำข้อมูลของลูกค้าไปใช้เพื่อประโยชน์ในการพัฒนาและนำเสนอบริการที่ตอบโจทย์ลูกค้าได้ดีขึ้น (GL2) และ
(2) สามารถกำกับดูแลผู้ให้บริการให้สามารถดูแลความเสี่ยงได้อย่างเหมาะสม ได้มาตรฐานเพื่อให้มั่นใจว่าการรับส่งข้อมูลของลูกค้ามีความปลอดภัยและมีการดูแลลูกค้าอย่างเหมาะสม (RL2)

ผู้ให้บริการที่รับข้อมูลของลูกค้าภายใต้หลักเกณฑ์ฉบับนี้ ได้แก่ ผู้ให้บริการที่สามารถนำข้อมูลของลูกค้าไปใช้เพื่อประโยชน์ในการพัฒนาและนำเสนอบริการที่ตอบโจทย์ลูกค้าได้ดีขึ้น โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล และได้รับการกำกับดูแลในด้านการเก็บรักษาและการรับส่งข้อมูลของลูกค้าที่ได้มาตรฐาน[16] ได้แก่

1) ผู้ให้บริการทางการเงินภายใต้การกำกับของ ธปท. ซึ่งประกอบด้วย สถาบันการเงิน และ SFIs ตาม พ.ร.บ. ธุรกิจสถาบันการเงิน ผู้ให้บริการการชำระเงิน และผู้ให้บริการสินเชื่อภายใต้การกำกับของ ธปท.

---

[13] หมายถึง ผู้ให้บริการสินเชื่อ รวมถึง ธพ. SFIs ผู้ให้บริการ personal loan ผู้ให้บริการ nano finance ผู้ให้บริการบัตรเครดิต และผู้ให้บริการ peer-to-peer lending platform

[14] คำนวณจากค่าเฉลี่ยของจำนวนบัญชีสินเชื่อ ณ สิ้นเดือน 12 เดือน และค่าเฉลี่ยของยอดสินเชื่อคงค้าง ณ สิ้นเดือน 12 เดือน (12-month average) นับย้อนขึ้นไปจากเดือนที่หลักเกณฑ์มีผลบังคับใช้ ทั้งนี้ ให้ถือปฏิบัติตามเกณฑ์ไปตลอด แม้ว่าต่อมาจะมียอดที่คำนวณได้ลดลงต่ำกว่า threshold ที่กำหนด

[15] ตามข้อ 3.1 1) และ 2)

[16] ตัวอย่างของประเทศที่ใช้แนวทางนี้ได้แก่ อินเดีย ออสเตรเลีย และสหราชอาณาจักร

ที่จะสามารถนำข้อมูลที่ได้รับจากลูกค้าไปใช้ประโยชน์ในการพัฒนาและนำเสนอบริการทางการเงินของผู้ให้บริการรายนั้น ๆ ที่ตอบโจทย์การเข้าถึงสินเชื่อในระบบอย่างเหมาะสมและการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคลก่อน

2) ผู้ให้บริการอื่น ๆ ที่ได้รับการกำกับดูแลภายใต้หลักเกณฑ์ที่มีมาตรฐานในระดับเดียวกัน โดยในระยะแรกจะมุ่งเน้นไปที่ผู้ให้บริการทางการเงินภายใต้การกำกับของ ก.ล.ต. และ คปภ. ซึ่งทั้งสองหน่วยงานอยู่ระหว่างการพิจารณาหลักเกณฑ์และแนวทางการกำกับดูแลการรับส่งข้อมูลให้สอดคล้องกัน ทั้งนี้ ในอนาคตสามารถขยายขอบเขตผู้ให้บริการที่รับข้อมูลในภาคสถาบันการเงินไปยังผู้ให้บริการในภาคส่วนอื่นที่ได้รับการกำกับภายใต้หลักเกณฑ์ที่มีมาตรฐานในระดับเดียวกันได้ต่อไป

ทั้งนี้ ในกรณีที่ผู้ให้บริการที่รับข้อมูลมีข้อมูลของลูกค้าอยู่ด้วย ควรจัดทำกลไกให้ลูกค้าใช้สิทธิส่งข้อมูลดังกล่าวไปยังผู้ให้บริการรายอื่นได้ด้วย เพื่อให้พร้อมทำหน้าที่ทั้งในฐานะผู้ส่งข้อมูลและผู้รับข้อมูล (ตามหลัก reciprocity)[17]

อนึ่ง เนื่องจากการให้บริการรวบรวมและบริหารจัดการข้อมูลภายใต้ consent ของลูกค้าในฐานะบุคคลที่สาม (Third Party Data Aggregator) จำเป็นที่จะต้องมีเกณฑ์การกำกับดูแลเพิ่มเติม เพื่อให้มั่นใจได้ว่าการให้บริการมีความปลอดภัยและได้มาตรฐาน ธปท. จะพิจารณากำหนดแนวทางการอนุญาตและกำกับดูแล Third Party Data Aggregator เพิ่มเติมต่อไป โดยจะพิจารณาให้สอดรับกับกรอบระยะเวลาที่คาดว่าจะเริ่มให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลของตนในภาคสถาบันการเงินได้ภายในปี 2569

3.3 หลักการในการกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล

> ***หลักการ:*** *หลักการในการกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูลต้องพิจารณาถึง*
> *(1) การส่งเสริมการใช้สิทธิของลูกค้า โดยเงื่อนไขและค่าธรรมเนียมต้องไม่เป็นอุปสรรคต่อลูกค้าในการใช้งานและต่อผู้ให้บริการในการเข้าร่วมรับส่งข้อมูล (GL1 และ RL1.1) และ*
> *(2) ไม่ทำให้เกิดการรับส่งข้อมูลเกินความจำเป็น (RL1.2)*

ในการกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล ผู้ให้บริการต้องปฏิบัติตามหลักการดังนี้[18]

1) เงื่อนไขที่เกี่ยวข้องกับการรับส่งข้อมูล: ผู้ให้บริการต้องไม่กำหนดเงื่อนไขหรือมีการดำเนินการที่เป็นอุปสรรคต่อการรับส่ง หรือต่อการใช้ประโยชน์ข้อมูล เช่น ขั้นตอนการเข้าร่วมหรือการใช้งานที่มีความยุ่งยาก การจำกัดระยะเวลาหรือจำนวนครั้งในการใช้งานไว้น้อยเกินไปจนเป็นอุปสรรค

---

[17] คณะทำงานที่ประกอบด้วยผู้แทนจากผู้ให้บริการและหน่วยงานต่างๆ ที่เกี่ยวข้องอยู่ระหว่างกำหนดแนวปฏิบัติที่จะใช้ร่วมกันในการเข้าร่วมและรับส่งข้อมูลภายใต้หลักเกณฑ์นี้ ซึ่งรวมถึงเงื่อนไขการเข้าร่วมของผู้ให้บริการที่มีข้อมูลของลูกค้า ที่ควรทำหน้าที่ทั้งฐานะทั้งผู้รับและผู้ส่งข้อมูลด้วย

[18] ธปท. จะหารือร่วมกับผู้ให้บริการและผู้ที่เกี่ยวข้องในคณะกรรมการขับเคลื่อนและคณะทำงาน (working group) โครงการ Your Data เพื่อกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล ซึ่งรวมถึง threshold ที่เป็นระดับการใช้งานปกติในรายละเอียดต่อไป

2) ค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล: โดยทั่วไป ไม่ให้ผู้ให้บริการคิดค่าธรรมเนียมที่เกี่ยวข้องกับการใช้สิทธิรับส่งข้อมูลของลูกค้าตามเกณฑ์นี้ เนื่องจากเป็นสิทธิของเจ้าของข้อมูล[19] เว้นแต่ในกรณีที่มีการเรียกข้อมูลสูงเกินกว่าระดับปกติที่กำหนด (Threshold) ผู้ให้บริการที่ส่งข้อมูลอาจคิดค่าธรรมเนียมจากผู้ให้บริการที่รับข้อมูลได้ เพื่อไม่ให้มีการเรียกข้อมูลเกินความจำเป็น และหากการเรียกข้อมูลเกินกว่าระดับปกตินั้นเกิดจากตัวลูกค้า ผู้ให้บริการที่รับข้อมูลอาจเรียกเก็บค่าธรรมเนียมกับลูกค้าได้[20] โดยค่าธรรมเนียมที่เรียกเก็บต้องไม่สูงเกินไปจนเป็นอุปสรรคต่อการใช้สิทธิของลูกค้า ซึ่งจะกำหนดร่วมกันในคณะกรรมการขับเคลื่อนและคณะทำงาน รวมทั้งต้องถือปฏิบัติตามหลักเกณฑ์ ธปท. ที่เกี่ยวข้อง[21] ซึ่งรวมถึงการเปิดเผยข้อมูลค่าธรรมเนียมดังกล่าวให้ลูกค้าทราบด้วย

3.4 การกำกับดูแลด้านการคุ้มครองผู้บริโภคและการรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและปลอดภัย

> ***หลักการ**: แนวทางการกำกับดูแลด้านการคุ้มครองผู้บริโภคและการรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและปลอดภัย ต้องพิจารณา*
> *(1) ให้มีการคุ้มครองผู้บริโภคและการบริหารจัดการความเสี่ยงได้อย่างเหมาะสม (RL2) และ*
> *(2) ไม่เป็นภาระและต้นทุนต่อผู้ให้บริการมากจนเกินไป และไม่กลายเป็นเงื่อนไขที่จะเป็นอุปสรรคต่อการรับส่งข้อมูล (RL1 และ GL3)*

ธปท. กำหนดแนวทางกำกับดูแลด้านการคุ้มครองผู้บริโภค ความเป็นส่วนบุคคลของข้อมูล และการรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและการบริหารจัดการข้อมูลให้มีความปลอดภัย เพื่อให้ลูกค้ามีความมั่นใจในการใช้สิทธิส่งข้อมูลทั้งก่อน ระหว่าง และหลังจากการใช้สิทธิ ซึ่งสอดคล้องกับแนวทางในต่างประเทศ[22] ดังนี้

1) การคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูล: ผู้ให้บริการที่เป็นผู้ส่งหรือรับข้อมูลต้อง

1.1) ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูล เช่น PDPA และหลักเกณฑ์ ธปท. ว่าด้วยเรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม

---

[19] ซึ่งสอดคล้องกับแนวทางของหลายประเทศ อาทิ สหราชอาณาจักร และออสเตรเลีย

[20] ตัวอย่างประเทศที่มีแนวทางป้องกันกรณีลูกค้าขอให้เรียกข้อมูลเกินกว่าระดับปกติ เช่น ในประเทศบราซิล สถาบันการเงินสามารถกำหนดเพดานจำนวนธุรกรรมต่อนาทีหรือต่อวินาทีที่ลูกค้าจะขอให้ส่งข้อมูลได้ ขณะที่ในประเทศสหรัฐอาหรับเอมิเรตส์ กำหนดให้ผู้ให้บริการสามารถคิดค่าธรรมเนียมกับลูกค้าได้ในกรณีที่ลูกค้าขอให้ผู้ให้บริการเรียกข้อมูล (1) เกินกว่า 15 API Calls ต่อวัน สำหรับการรับส่งข้อมูลทั่วไป และ (2) เกินกว่า 5 API calls ต่อวัน สำหรับการอัปเดตข้อมูลอัตโนมัติ ซึ่งปริมาณข้อมูลที่ส่งจาก API Call ในแต่ละครั้งเป็นไปตามที่ผู้ให้บริการตกลงกันใน UAE's Open Finance Business Rules (ปัจจุบันกำหนดให้ 1 API Call สามารถรับส่งข้อมูลได้สูงสุด 100 รายการ) (https://openfinanceuae.atlassian.net/wiki/spaces/OF/pages/124846096/Commercial+and+Pricing+Model)

[21] เช่น ประกาศ ธปท. ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ซึ่งกำหนดให้ผู้ให้บริการต้องกำหนดค่าธรรมเนียมอย่างเป็นธรรม คำนึงถึงต้นทุนที่แท้จริง ไม่เอาเปรียบลูกค้า ไม่ร่วมกับผู้ให้บริการอื่นในการกำหนดราคา ลักษณะ และเงื่อนไขที่ทำให้ลูกค้าเสียประโยชน์ เป็นต้น

[22] สอดคล้องกับแนวทางการกำกับดูแลในต่างประเทศ เช่น บราซิล สหรัฐอาหรับเอมิเรตส์ ออสเตรเลีย ได้กำหนดหลักเกณฑ์กำกับดูแลการรับส่งข้อมูลตั้งแต่ก่อน ระหว่าง และหลังการใช้สิทธิของลูกค้า เช่น การดำเนินการเกี่ยวกับ consent การยืนยันตัวตน และการยืนยันการใช้สิทธิก่อนการส่งข้อมูล กำหนดให้การส่งข้อมูลทำตามมาตรฐานที่กำหนด และมีการคุ้มครองผู้บริโภคให้สามารถบริหารจัดการสิทธิของตนได้ง่าย มีการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศของข้อมูลที่เพียงพอ รวมถึงสามารถร้องเรียนเมื่อเกิดปัญหา

ตัวอย่างกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในเรื่องการคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูล

(1) PDPA กำหนดหลักการจัดการข้อมูลส่วนบุคคลกรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐาน consent ไว้เบื้องต้น เช่น ผู้ให้บริการต้องได้รับ consent จากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะที่เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งต้องทำโดยชัดแจ้ง ต้องแจ้งวัตถุประสงค์และแยกส่วนจากข้อความอื่นโดยชัดเจน โดยต้องมีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์ ทั้งนี้ ต้องทำให้สามารถถอน consent ได้ง่ายเช่นเดียวกับการให้ consent

(2) หลักเกณฑ์ ธปท.[23] ว่าด้วยเรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรมและหลักเกณฑ์ตามกฎหมายว่าด้วยระบบการชำระเงินและกฎหมายกำกับดูแลผู้ประกอบธุรกิจ Non-Bank แต่ละประเภท โดย ธปท. ได้กำหนดหลักเกณฑ์การดูแลข้อมูลของลูกค้าให้ผู้ให้บริการแต่ละประเภทถือปฏิบัติ เช่น การเปิดเผยข้อมูลลูกค้าให้แก่บุคคลอื่นต้องมีกระบวนการที่ทำให้มั่นใจว่าผู้รับข้อมูลสามารถรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้าได้อย่างรัดกุม เก็บข้อมูลของลูกค้าเท่าที่จำเป็น และใช้ข้อมูลตามวัตถุประสงค์ที่ลูกค้าให้ไว้ ผู้ให้บริการต้องรักษาข้อมูลของลูกค้าไว้เป็นความลับ โดยการเปิดเผยข้อมูลต้องเป็นไปตามกฎหมายที่เกี่ยวข้องหรือเมื่อได้รับ consent จากลูกค้า และมีช่องทางให้ลูกค้าสามารถถอน consent ได้สะดวก

(3) หลักเกณฑ์ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน[24] กำหนดให้ผู้ให้บริการต้องดำเนินการระบุและพิสูจน์ทราบตัวตนของลูกค้าให้เหมาะสมกับความเสี่ยงของผลิตภัณฑ์หรือบริการ ซึ่ง ธปท. ได้มีการกำหนดหลักเกณฑ์เพิ่มเติมสำหรับธุรกรรมการเปิดบัญชีเงินฝากและ e-money[25]

1.2) ปฏิบัติตามหลักเกณฑ์ที่ ธปท. กำหนดเพิ่มเติม ในส่วนของการคุ้มครองความเป็นส่วนบุคคลของข้อมูลตลอดกระบวนการใช้สิทธิส่งข้อมูล เพื่อป้องกันการเรียกหรือใช้ข้อมูลโดยไม่ได้รับ consent จากลูกค้า หรือการเกิดกรณีที่ผู้ที่ใช้สิทธิไม่ใช่ลูกค้าจริง ดังต่อไปนี้

---

[23] ประกอบด้วย

(1) เกณฑ์สำหรับผู้ประกอบธุรกิจสถาบันการเงิน SFIs และ Non-Bank ได้แก่ เอกสารแนบ 6 ของประกาศ ธปท. ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม ในส่วนมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้า

(2) เกณฑ์กำกับดูแลผู้ให้บริการการชำระเงิน ได้แก่ ประกาศ ธปท. ว่าด้วยหลักเกณฑ์ทั่วไปในการกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ในส่วนของการคุ้มครองผู้ใช้บริการ

(3) เกณฑ์กำกับดูแล Non-Bank ซึ่งมีข้อกำหนดให้ถือปฏิบัติเพิ่มเติมจากเกณฑ์ Market Conduct ในส่วนของการปฏิบัติและการจัดการเกี่ยวกับข้อมูลของผู้บริโภคตามเอกสารแนบว่าด้วยการดูแลผู้บริโภคตามประกาศ ธปท. จำนวน 4 ฉบับ ได้แก่ เอกสารแนบ 3 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบัตรเครดิต เอกสารแนบ 4 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ เอกสารแนบ 3 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ และเอกสารแนบ 4 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล (peer-to-peer lending platform)

[24] กฎกระทรวงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า พ.ศ. 2563 และประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน เรื่อง แนวทางในการระบุตัวตนและพิสูจน์ทราบตัวตนของลูกค้าและการระบุและพิสูจน์ทราบตัวตนของผู้ได้รับผลประโยชน์ที่แท้จริง

[25] ประกาศ ธปท. ว่าด้วยหลักเกณฑ์การรู้จักลูกค้าสำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน ประกาศ ธปท. ว่าด้วยหลักเกณฑ์การรับฝากเงินหรือการรับเงินจากประชาชนของสถาบันการเงินเฉพาะกิจ และประกาศ ธปท. ว่าด้วยหลักเกณฑ์การรู้จักลูกค้าสำหรับการเปิดใช้บริการเงินอิเล็กทรอนิกส์

1.2.1) การขอ consent จากลูกค้า เพื่อให้ผู้ให้บริการที่ส่งข้อมูลสามารถส่งข้อมูลไปยังผู้ให้บริการที่รับข้อมูลได้ โดยอย่างน้อยต้อง

(1) แยกข้อความการขอ consent ให้ส่งข้อมูลของลูกค้าภายใต้หลักเกณฑ์ฉบับนี้ออกจากข้อความอื่น และการขอ consent ในเรื่องอื่น ๆ อย่างชัดเจน

(2) แจ้งข้อมูลและเงื่อนไขแก่ลูกค้าที่เพียงพอต่อการพิจารณาตัดสินใจใช้สิทธิส่งข้อมูล[26] โดยอย่างน้อยต้องประกอบด้วย

(2.1) ประเภทและรายการข้อมูลที่ขอให้ลูกค้าให้ consent

(2.2) วัตถุประสงค์การใช้ข้อมูล โดยต้องเป็นไปเพื่อการให้บริการหรือการทำธุรกรรมที่ลูกค้าให้ consent และต้องอยู่ภายใต้ขอบเขตธุรกิจที่กำหนดในกฎหมายกำกับดูแลธุรกิจหรือได้รับอนุญาตจากหน่วยงานกำกับดูแลของตนเท่านั้น

(2.3) ระยะเวลาการขอ consent ซึ่งต้องสอดคล้องกับวัตถุประสงค์การใช้ข้อมูล โดยอาจขอ consent เพื่อรองรับการเรียกข้อมูลของลูกค้าสำหรับครั้งเดียว หรือเป็นช่วงระยะเวลาก็ได้[27] ทั้งนี้ ในกรณีที่ขอ consent เป็นช่วงระยะเวลา ต้องมีกำหนดระยะเวลาไม่เกิน 12 เดือน[28] เพื่อให้ลูกค้าได้ทบทวนความจำเป็นและความเหมาะสมของการให้ consent ดังกล่าว

(2.4) รายชื่อผู้ให้บริการที่จะใช้ข้อมูลดังกล่าวเพื่อให้บริการแก่ลูกค้า

(2.5) รายชื่อผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูลของลูกค้าในส่วนของผู้ให้บริการที่รับข้อมูล เช่น บุคคลภายนอกที่ผู้ให้บริการว่าจ้างมาทำหน้าที่เก็บรวบรวม และ/หรือประมวลผลข้อมูลของลูกค้า หรือช่วยเชื่อมต่อกับระบบหรือผู้ให้บริการรายอื่นเพื่อรับส่งข้อมูลตาม consent ของลูกค้า

1.2.2) ผู้ให้บริการที่ส่งข้อมูลต้องมีกระบวนการให้ลูกค้ายืนยันตัวตน (authentication) และยืนยันการใช้สิทธิส่งข้อมูล (authorization) ก่อนที่จะส่งข้อมูลให้แก่ผู้ให้บริการตามข้อ 1.2.1) หลังจากได้รับคำร้องขอพร้อม consent เพื่อให้มั่นใจได้ว่าลูกค้าเป็นผู้ใช้สิทธิและต้องการใช้สิทธิจริง โดย

(1) ให้ลูกค้าทำ authentication ด้วยระดับ Authenticator Assurance Level ที่ AAL2[29] หรือ 2 Factor-Authentication (เช่น ใช้ PIN และ OTP)[30] ซึ่งเป็นระดับที่ไม่สูงเกินไปจนเป็นอุปสรรคต่อการใช้สิทธิของลูกค้า และไม่ต่ำเกินไปจนทำให้เกิดความเสี่ยงที่ผู้ทำธุรกรรมไม่ใช่ลูกค้าจริง

---

[26] สอดคล้องกับข้อกำหนดของบราซิล ออสเตรเลีย และสหรัฐอาหรับเอมิเรตส์

[27] Consent แบบช่วงระยะเวลา มักพบเห็นในผลิตภัณฑ์ทางการเงินที่ช่วยบริหารจัดการทางการเงินที่เหมาะสมกับพฤติกรรมของลูกค้าแต่ละบุคคล เช่น ลูกค้าให้ consent ไว้เป็นเวลา 12 เดือนเพื่อส่งข้อมูลบัญชีของตนที่อยู่กับผู้ให้บริการหลาย ๆ รายมาแสดงในแอปพลิเคชันมือถือเดียวได้ตลอดระยะเวลา 12 เดือนที่ให้ consent ไว้ เพื่อวางแผนรายรับรายจ่าย การออม การลงทุน

[28] สอดคล้องกับเกณฑ์ของบราซิล ออสเตรเลีย และสหรัฐอาหรับเอมิเรตส์ ที่กำหนดให้ consent เป็นช่วงระยะเวลา ต้องมีกำหนดระยะเวลาไม่เกิน 12 เดือน

[29] สอดคล้องกับแนวทางของสหราชอาณาจักร และออสเตรเลีย

[30] ปัจจุบัน 2-Factor Authentication ใช้กับการโอนเงินและชำระเงินมูลค่าต่ำกว่า 50,000 บาทต่อครั้ง

(2) ให้ลูกค้าทำ authorization ก่อนการส่งข้อมูล โดย

(2.1) แยกข้อความการขอ authorization ภายใต้หลักเกณฑ์ฉบับนี้ออกจากข้อความอื่น และการขอ authorization ในเรื่องอื่น ๆ อย่างชัดเจน

(2.2) แจ้งข้อมูลและเงื่อนไขแก่ลูกค้าที่เพียงพอต่อการพิจารณาตัดสินใจให้ authorization ในลักษณะเดียวกับการขอ consent ในข้อ 1.2.1 (2.1) และ (2.2) กำหนดระยะเวลาการให้ authorization ที่เหมาะสมกับวัตถุประสงค์และสอดคล้องกับระยะเวลาการให้ consent และแจ้งรายชื่อผู้ให้บริการที่จะเป็นผู้ส่งข้อมูล รวมถึงต้องแจ้งรายชื่อผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูลของลูกค้าในส่วนของผู้ให้บริการที่ส่งข้อมูลด้วย

1.2.3) ผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลต้องดำเนินการให้ลูกค้าสามารถบริหารจัดการและตรวจสอบ consent และ authorization ได้ง่ายและสะดวก รวมถึงแจ้งผู้ที่เกี่ยวข้องทราบถึงการดำเนินการดังกล่าว ดังนี้

(1) ผู้ให้บริการต้องให้หลักฐานการให้ การแก้ไข และการถอน consent และ authorization แก่ลูกค้าไว้เป็นหลักฐานตามช่องทางที่ลูกค้าได้แจ้งไว้แก่ผู้ให้บริการ เช่น email แอปพลิเคชัน หรือช่องทางให้บริการของผู้ให้บริการ เพื่อให้ลูกค้าสามารถตรวจสอบได้

(2) ผู้ให้บริการต้องจัดให้มีช่องทางให้ลูกค้าบริหารจัดการ consent และ authorization ได้ง่ายและสะดวก เพื่อรองรับการเปลี่ยนแปลง การยกเลิก และการตรวจสอบประวัติการให้ consent และ authorization

(3) ผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลต้องแจ้งให้ลูกค้าและผู้ให้บริการอีกฝ่ายทราบเมื่อ consent หรือ authorization มีการเปลี่ยนแปลง ยกเลิก หรือหมดอายุแล้วแต่กรณี เพื่อไม่ให้มีการเรียก ใช้ หรือส่งข้อมูลโดยไม่มี consent ของลูกค้ารองรับ และกรณีที่ consent หรือ authorization ยังมีผลบังคับใช้อยู่ ให้ผู้ให้บริการแจ้งเตือนให้ลูกค้าทราบถึงการมีอยู่ของ consent และ authorization ดังกล่าวอย่างน้อยทุก 90 วัน[31]

ทั้งนี้ ธปท. จะกำหนดแนวปฏิบัติในเรื่อง consent และ authorization ร่วมกับผู้ที่เกี่ยวข้องผ่านคณะกรรมการขับเคลื่อนและคณะทำงานต่อไป

2) การรับส่งข้อมูลให้เป็นไปตามมาตรฐานกลางและการบริหารจัดการข้อมูลให้มีความปลอดภัย

2.1) ผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลต้องปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติที่ ธปท. กำหนด ซึ่งรวมถึงรูปแบบและกระบวนการเกี่ยวกับ consent authentication และ authorization ลักษณะการออกแบบการใช้งานที่สะดวกและสร้างประสบการณ์ที่ดีแก่ลูกค้า (customer experience) รูปแบบการเชื่อมต่อ การเก็บ และการรับส่งข้อมูล รวมทั้งการดูแลแก้ไขเมื่อเกิดปัญหา เป็นต้น โดยในการจัดทำมาตรฐานกลางและแนวปฏิบัติ ธปท. จะหารือร่วมกับผู้ที่เกี่ยวข้องผ่านคณะกรรมการขับเคลื่อน

[31] สอดคล้องกับหลักเกณฑ์ Consumer Data Right ของออสเตรเลียและ Customer Experience Guideline ของ UK Open Banking

และคณะทำงานโครงการ Your Data โดย ธปท. จะนำมาตรฐานกลางและแนวปฏิบัติที่จัดทำร่วมกับผู้ที่เกี่ยวข้องมาบังคับใช้ต่อไป

2.2) ผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลต้องมีการบริหารจัดการข้อมูลที่ดี เพื่อให้ข้อมูลของลูกค้ามีความปลอดภัยตลอดทั้งกระบวนการ โดยครอบคลุมถึงการกำกับดูแลกิจการให้มีธรรมาภิบาลในการบริหารจัดการข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูลในด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการเมื่อเกิดเหตุผิดปกติหรือปัญหาเกี่ยวกับข้อมูล ดังนี้

2.2.1) การกำกับดูแลกิจการให้มีธรรมาภิบาลในการบริหารจัดการข้อมูล: ผู้ให้บริการต้องมีการกำกับดูแลกิจการด้านธรรมาภิบาลในการบริหารจัดการข้อมูลเพื่อให้มั่นใจว่าข้อมูลที่ผู้ให้บริการรับส่งและขั้นตอนต่าง ๆ ที่เกี่ยวข้องมีการดูแลด้านความปลอดภัยและความเป็นส่วนบุคคลของข้อมูลตลอดกระบวนการ ดังนี้

(1) คณะกรรมการของผู้ให้บริการต้องให้ความสำคัญกับการใช้สิทธิในข้อมูลของลูกค้า การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล และทำหน้าที่กำกับดูแลให้มีการดำเนินการในเรื่องนี้อย่างเคร่งครัดและต่อเนื่อง โดย

(1.1) กำหนดและอนุมัตินโยบายที่ให้ความสำคัญกับการใช้สิทธิส่งข้อมูลของลูกค้า การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ซึ่งครอบคลุมการบริหารจัดการตลอดวงจรชีวิตข้อมูล และทบทวนนโยบายดังกล่าวตามความถี่ที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(1.2) รับผิดชอบในการกำกับดูแลในภาพรวม และกำกับดูแลให้มีโครงสร้างองค์กรที่สามารถรองรับการดำเนินการให้ลูกค้าใช้สิทธิส่งข้อมูลของลูกค้าได้อย่างเป็นรูปธรรม มีการสอบทานและถ่วงดุลการปฏิบัติงานอย่างเหมาะสม โดยพิจารณารูปแบบและแนวทางการดำเนินการให้เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของผู้ให้บริการ

(1.3) กำกับดูแลให้ผู้บริหารระดับสูง (i) นำนโยบายดังกล่าวไปสื่อสารให้ผู้ที่เกี่ยวข้องภายในองค์กรตระหนักถึงความสำคัญและเข้าใจบทบาทหน้าที่ความรับผิดชอบ และ (ii) ผลักดันให้ผู้ที่เกี่ยวข้องดำเนินการตามนโยบายที่กำหนดอย่างเคร่งครัดและต่อเนื่อง

(1.4) กำกับดูแลให้เกิดการจัดสรรทรัพยากร เพื่อสนับสนุนการดำเนินการด้านการใช้สิทธิส่งข้อมูลของลูกค้า การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้ได้ผลสัมฤทธิ์ตามที่กำหนดไว้

(1.5) ติดตามและกำกับดูแลภาพรวมการดำเนินการให้ลูกค้าใช้สิทธิส่งข้อมูล การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามหลักเกณฑ์ที่เกี่ยวข้องและนโยบายที่กำหนด โดยกำกับดูแลให้ฝ่ายจัดการ (i) มีการรายงานการดำเนินงานและความเสี่ยงต่อผู้บริหาร

ระดับสูงอย่างสม่ำเสมอ และต่อคณะกรรมการอย่างน้อยปีละครั้ง เพื่อใช้ประกอบการพิจารณาทบทวนนโยบายและแผนกลยุทธ์ในส่วนที่เกี่ยวข้อง รวมทั้ง (ii) มีการรายงานความเสี่ยงที่สำคัญและประเด็นที่อาจส่งผลอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ให้บริการต่อคณะกรรมการโดยไม่ชักช้า เพื่อพิจารณาสั่งการป้องกันหรือให้มีการแก้ไขปัญหาสำคัญในเวลาที่เหมาะสม

ทั้งนี้ เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการปฏิบัติงาน คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดย่อยหรือผู้ที่ได้รับมอบหมายดำเนินการ ดังนี้ (ก) ทบทวนนโยบายแทนคณะกรรมการ โดยต้องมีการรายงานคณะกรรมการทราบ และหากมีการเปลี่ยนแปลงที่มีนัยสำคัญ ต้องเสนอคณะกรรมการพิจารณาอนุมัติด้วย (ข) ดูแลการจัดโครงสร้างองค์กรและการกำหนดบทบาทหน้าที่ในรายละเอียดตามโครงสร้างองค์กรในภาพรวมที่คณะกรรมการได้เคยอนุมัติไว้แล้ว (ค) ติดตามการรายงานการดำเนินงานและประเด็นความเสี่ยงสำคัญจากฝ่ายจัดการ โดยต้องรายงานสรุปภาพรวมการดำเนินงานให้คณะกรรมการทราบอย่างน้อยปีละครั้ง และรายงานประเด็นความเสี่ยงสำคัญต่อคณะกรรมการโดยไม่ชักช้า

ในกรณีที่มีการมอบหมายข้างต้น คณะกรรมการต้องกำหนดบทบาทหน้าที่ ความรับผิดชอบ และอำนาจของคณะกรรมการชุดย่อยหรือผู้ที่รับผิดชอบดังกล่าวให้ชัดเจน และต้องติดตามภาพรวมการดำเนินงานและประเด็นความเสี่ยงสำคัญที่ได้รับรายงานจากคณะกรรมการชุดย่อยหรือผู้ที่รับผิดชอบที่ได้รับมอบหมายจากคณะกรรมการอย่างสม่ำเสมอ เพื่อกำกับดูแลผู้ให้บริการให้สามารถดำเนินการปรับปรุงแก้ไขกรณีที่เกิดปัญหาได้อย่างเหมาะสมและทันการณ์ รวมทั้งมีการพิจารณาสาเหตุของปัญหาและปรับปรุงเพื่อป้องกันมิให้เกิดปัญหาซ้ำอีกในอนาคต

(2) ผู้บริหารระดับสูงของผู้ให้บริการต้องทำหน้าที่ผลักดันและดูแลให้มีการดำเนินการตามนโยบายที่ได้รับอนุมัติจากคณะกรรมการอย่างเคร่งครัดและต่อเนื่อง โดย

(2.1) นำนโยบายที่ได้รับอนุมัติจากคณะกรรมการไปสื่อสารและผลักดันให้ผู้ที่เกี่ยวข้องในองค์กรมีการดำเนินการตามนโยบายดังกล่าวอย่างเป็นรูปธรรมและเคร่งครัด

(2.2) จัดให้มีโครงสร้างองค์กร กำหนดผู้รับผิดชอบและบทบาทหน้าที่ในรายละเอียดที่ชัดเจนตามโครงสร้างองค์กรที่คณะกรรมการได้เคยอนุมัติไว้แล้ว และผลักดันให้เกิดการจัดสรรทรัพยากรอย่างเพียงพอที่จะสนับสนุนการดำเนินการด้านการใช้สิทธิส่งข้อมูลของลูกค้า การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้ได้ผลสัมฤทธิ์ตามที่กำหนดไว้

(2.3) ติดตามการดำเนินการเรื่องการให้ลูกค้าใช้สิทธิส่งข้อมูล การรักษาความปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามนโยบายที่คณะกรรมการกำหนดและหลักเกณฑ์ที่หน่วยงานกำกับดูแลกำหนดในส่วนที่เกี่ยวข้อง รวมทั้งมีการรายงานเรื่องดังกล่าวต่อคณะกรรมการ คณะกรรมการชุดย่อย หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอย่างน้อยปีละครั้ง และมี

การรายงานความเสี่ยงที่สำคัญและประเด็นที่อาจส่งผลอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ให้บริการต่อคณะกรรมการโดยไม่ชักช้า

ทั้งนี้ ผู้ให้บริการที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศหรือของผู้ให้บริการทางการเงินต่างประเทศในประเทศไทย ให้ถือปฏิบัติเฉพาะส่วนของผู้บริหารระดับสูงของผู้ให้บริการตามข้อ 2.2.1 (2)

2.2.2) การรักษาความปลอดภัยของข้อมูลในด้านเทคโนโลยีสารสนเทศ (IT): ผู้ให้บริการต้องมีการบริหารจัดการด้าน IT ให้มีความมั่นคงปลอดภัย สามารถดูแลข้อมูลของลูกค้าได้อย่างเหมาะสม และสามารถป้องกันและรับมือเหตุการณ์ภัยคุกคามไซเบอร์และข้อมูลรั่วไหลได้อย่างมีประสิทธิภาพ โดยปฏิบัติตามมาตรฐานขั้นต่ำเรื่องการรักษาความปลอดภัยของข้อมูลในด้าน IT ที่ ธปท. กำหนด[32] (รายละเอียดตามเอกสารแนบ) อาทิ

- การบริหารจัดการทรัพย์สินด้าน IT อย่างเหมาะสม
- การรักษาความมั่นคงปลอดภัยของข้อมูลตลอดวงจรชีวิตของข้อมูล
- การควบคุมการเข้าถึงเพื่อป้องกันการเข้าถึงระบบงานและข้อมูลของลูกค้าโดยไม่ได้รับอนุญาต
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน
- การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบ IT
- การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม
- การจัดหาและพัฒนาระบบอย่างปลอดภัยตามมาตรฐานสากล
- การบริหารความเสี่ยงจากบุคคลภายนอก
- การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของลูกค้าย้อนหลัง (audit trail) และการจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) เพื่อตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของลูกค้าย้อนหลัง อันจะเป็นประโยชน์ในการดำเนินคดีและระบุตัวผู้กระทำผิด และ/หรือผู้รับผิดชอบกรณีเกิดการละเมิดข้อมูลของลูกค้าหรือเกิดข้อมูลรั่วไหล[33]

2.2.3) การบริหารจัดการเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาเกี่ยวกับข้อมูล: ผู้ให้บริการต้องมีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้สิทธิส่งข้อมูลของลูกค้า

---

[32] ธพ. SFIs และผู้ให้บริการการชำระเงินที่มีนัยสำคัญ ต้องปฏิบัติตามมาตรฐานขั้นต่ำดังกล่าวอยู่แล้ว ส่วนผู้ให้บริการการชำระเงินรายที่ไม่มีนัยสำคัญและผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงิน (Non-Bank) ต้องถือปฏิบัติเพิ่มเติมเพื่อให้เป็นไปตามมาตรฐานดังกล่าว ทั้งนี้ คุณสมบัติของผู้ให้บริการการชำระเงินรายที่มีนัยสำคัญเป็นไปตามที่กำหนดในข้อ 3.2 (3) ตามประกาศธนาคารแห่งประเทศไทย ที่ สนช. 1/2564 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน

[33] ธปท. จะร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแนวปฏิบัติเรื่องการกำหนดความรับผิดในรายละเอียดต่อไป

เช่น ข้อมูลรั่วไหล การถูกโจมตีจากภัยคุกคามทางไซเบอร์ อย่างเหมาะสมและทันท่วงที ทั้งในด้านระบบเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านปฏิบัติการอื่น ๆ[34] ดังนี้

(1) มีกระบวนการที่รัดกุมในการรับมือและตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาให้สอดคล้องกับระดับความเสี่ยง เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสมและทันการณ์ และมีการแก้ไขปัญหาโดยไม่ชักช้า ตลอดจนมีแนวทางในการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ รวมทั้งมีแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติหรือมิให้เกิดปัญหาซ้ำอีกในอนาคต

(2) มีการรายงานเหตุการณ์ผิดปกติหรือปัญหาต่อผู้บริหารระดับสูง และ/หรือคณะกรรมการที่เกี่ยวข้องที่เหมาะสมกับระดับความเสี่ยง โดยในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่รุนแรงหรืออาจส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ให้บริการ ต้องมีการรายงานให้คณะกรรมการของผู้ให้บริการทราบอย่างทันท่วงทีด้วย

(3) มีการแก้ไขปัญหาและจัดการเรื่องร้องเรียน โดยผู้ให้บริการภายใต้การกำกับของ ธปท. ต้องปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องกับการแก้ไขปัญหาและจัดการเรื่องร้องเรียนที่บังคับใช้อยู่แล้วในปัจจุบัน[35] ซึ่งครอบคลุมประเด็นสำคัญ เช่น การกำหนดให้มีบุคลากรที่ทำหน้าที่รับเรื่องร้องเรียนและช่องทางรับเรื่องร้องเรียนโดยแจ้งให้ลูกค้าทราบช่องทางดังกล่าว กำหนดให้มีกระบวนการรับและดำเนินการเกี่ยวกับปัญหาและเรื่องร้องเรียนที่เป็นมาตรฐาน มีการแก้ไขด้วยความเป็นธรรม มีการติดตามการแก้ไขปัญหาและเรื่องร้องเรียนอย่างสม่ำเสมอ มีมาตรการแก้ไขปัญหา เยียวยา หรือชดเชยให้แก่ลูกค้า รวมทั้งมีการป้องกันไม่ให้เกิดปัญหาหรือเรื่องร้องเรียนซ้ำอีก[36]

---

[34] ตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามกฎหมายว่าด้วยระบบการชำระเงิน

[35] ประกอบด้วย

(1) เกณฑ์สำหรับผู้ประกอบธุรกิจสถาบันการเงิน SFIs และ Non-Bank ได้แก่ เอกสารแนบ 7 มาตรฐานขั้นต่ำสำหรับการแก้ไขปัญหาและจัดการเรื่องร้องเรียน ของประกาศ ธปท. ว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct) ในส่วนมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้า ตามเอกสารแนบ 7

(2) เกณฑ์กำกับดูแล Non-Bank ซึ่งมีข้อกำหนดให้ถือปฏิบัติเพิ่มเติมจากเกณฑ์ Market Conduct ในส่วนของการปฏิบัติเมื่อมีข้อร้องเรียน ได้แก่ 1) เอกสารแนบ 3 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบัตรเครดิต 2) เอกสารแนบ 4 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ 3) เอกสารแนบ 3 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ และ 4) เอกสารแนบ 4 ของประกาศ ธปท. ว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล (peer-to-peer lending platform)

[36] ธพ. SFIs ผู้ให้บริการบัตรเครดิต ผู้ให้บริการ personal loan ผู้ให้บริการ nano finance ต้องปฏิบัติตามแนวทางที่กำหนดภายใต้ขอบเขตของหลักเกณฑ์ Market Conduct อยู่แล้ว อย่างไรก็ดี ปัจจุบัน ผู้ให้บริการการชำระเงิน และผู้ให้บริการ peer-to-peer lending platform มีข้อกำหนดเกี่ยวกับการจัดการเรื่องร้องเรียนที่เข้มข้นน้อยกว่าผู้ให้บริการประเภทอื่น จึงจะกำหนดให้ผู้ให้บริการกลุ่มดังกล่าวที่จะรับส่งข้อมูลตามหลักเกณฑ์ฉบับนี้ ต้องปฏิบัติตามข้อกำหนดว่าด้วยการแก้ไขและจัดการเรื่องร้องเรียนให้เทียบเท่าตามหลักเกณฑ์ Market Conduct สำหรับ Non-Bank ที่มียอดสินเชื่อคงค้างรวมต่ำกว่าระดับที่มีนัยสำคัญที่ธนาคารแห่งประเทศไทยประกาศกำหนด (ตามเอกสารแนบ 11 ของหลักเกณฑ์ Market Conduct ในส่วนการแก้ไขปัญหาจัดการเรื่องร้องเรียน)

ทั้งนี้ หากต่อมามีข้อกำหนดในเรื่องดังกล่าวบรรจุในหลักเกณฑ์ Market Conduct สำหรับผู้ให้บริการการชำระเงิน และผู้ให้บริการ peer-to-peer lending platform เป็นการเฉพาะ ให้ถือปฏิบัติตามหลักเกณฑ์ใหม่ต่อไป

ทั้งนี้ ในกรณีที่ผู้ให้บริการจะทำการรับส่งข้อมูลของลูกค้าตามหลักเกณฑ์ฉบับนี้ผ่านกลไกในรูปแบบอื่น ให้หารือ ธปท. ก่อน เพื่อให้แน่ใจว่าการรับส่งข้อมูลผ่านกลไกดังกล่าวเป็นไปตามข้อกำหนดภายใต้หลักเกณฑ์ฉบับนี้

3.5 กระบวนการกำกับดูแลผู้ให้บริการให้ได้มาตรฐาน

ธปท. จะกำกับดูแลผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลของลูกค้าตามหลักเกณฑ์ฉบับนี้ ให้ได้มาตรฐานอย่างต่อเนื่อง ตั้งแต่ก่อนเริ่มให้บริการรับส่งข้อมูลของลูกค้า ระหว่างการให้บริการ และเมื่อผู้ให้บริการเกิดปัญหาหรือข้อพิพาทกับลูกค้า เพื่อให้มั่นใจว่าการรับส่งและการบริหารจัดการข้อมูลของลูกค้ามีความปลอดภัยและได้มาตรฐาน เป็นไปตามหลักเกณฑ์ มาตรฐานกลาง และแนวปฏิบัติที่กำหนด ดังนี้

1) ก่อนการเริ่มให้บริการรับส่งข้อมูลของลูกค้า:

1.1) ผู้ให้บริการต้องผ่านการทดสอบการปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติที่กำหนด รวมทั้งผ่านการประเมินของ ธปท. ว่ามีความพร้อมและคุณสมบัติเป็นไปตามหลักเกณฑ์ของ ธปท. โดยที่ผู้ให้บริการที่เข้าข่ายเป็นผู้ให้บริการที่ส่งข้อมูลและผู้ให้บริการที่รับข้อมูลตามหลักเกณฑ์ฉบับนี้ต้อง

1.1.1) ยื่นเอกสารที่แสดงถึงความพร้อมและคุณสมบัติของผู้ให้บริการที่เป็นไปตามหลักเกณฑ์ มาตรฐานกลาง และแนวปฏิบัติที่กำหนดมายัง ธปท.[37]

1.1.2) เข้ารับการทดสอบการปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติที่ ธปท. กำหนดกับระบบทะเบียนผู้ให้บริการรับส่งข้อมูล[38] (ระบบทะเบียนฯ) หากผู้ให้บริการผ่านการพิจารณาของ ธปท. ตามข้อ 1.1.1) และผ่านการทดสอบการปฏิบัติตามมาตรฐานกลางและแนวปฏิบัติ จะได้รับการขึ้นทะเบียนเป็นสมาชิกในระบบทะเบียนฯ

1.2) ธปท. จะแสดงรายชื่อผู้ให้บริการที่เป็นสมาชิกในระบบทะเบียนฯ รวมถึงวันที่เริ่มให้บริการ เพื่อให้ผู้ให้บริการและลูกค้าทราบ บนช่องทางเว็บไซต์ของ ธปท.

2) ระหว่างการให้บริการรับส่งข้อมูลของลูกค้า

2.1) ผู้ให้บริการต้องส่งข้อมูล และ/หรือรายงานที่เกี่ยวข้องกับการให้บริการตามหลักเกณฑ์ฉบับนี้ ตามที่ ธปท. กำหนด หรือเมื่อ ธปท. ร้องขอ เพื่อประโยชน์ในการติดตามพัฒนาการการใช้งาน ปัญหาอุปสรรค และการกำกับดูแลการให้บริการ เช่น จำนวน consent ได้รับจากลูกค้าแยกตาม

---

[37] กรณีผู้ที่เข้าร่วมรับข้อมูลตามหลักเกณฑ์ฉบับนี้เป็นผู้ให้บริการภายใต้การกำกับดูแลของหน่วยงานอื่น หน่วยงานกำกับดูแลดังกล่าวมีหน้าที่ในการพิจารณาความพร้อมและคุณสมบัติของผู้ที่อยู่ภายใต้การกำกับดูแลของตนและแจ้งให้ผู้ให้บริการของระบบทะเบียนฯ ทราบ เพื่อประกอบการพิจารณารับขึ้นทะเบียน ทั้งนี้ ธปท. จะได้หารือกับหน่วยงานกำกับดูแลดังกล่าวเพื่อให้การพิจารณาความพร้อม คุณสมบัติ และการปฏิบัติตามหลักเกณฑ์ต่าง ๆ มีมาตรฐานในระดับเดียวกัน

[38] ธปท. อยู่ระหว่างพิจารณาผู้ให้บริการระบบทะเบียนฯ

วัตถุประสงค์การใช้ข้อมูล จำนวนครั้งการเรียกใช้ข้อมูล (อาทิ API calls) สัดส่วนการร้องขอข้อมูลที่สำเร็จและไม่สำเร็จ ปัญหาการให้บริการและเรื่องร้องเรียน

2.2) ธปท. มีการติดตามและกำกับดูแลผู้ให้บริการอย่างต่อเนื่อง โดยหากพบว่าระบบหรือการให้บริการตามหลักเกณฑ์ฉบับนี้มีปัญหาหรือข้อบกพร่อง อาจสั่งการให้ผู้ให้บริการดำเนินการแก้ไข กรณีที่ผู้ให้บริการไม่ได้ดำเนินการปรับปรุงหรือแก้ไขปัญหาหรือข้อบกพร่องภายในระยะเวลาที่กำหนด ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อฐานะหรือการดำเนินงานของผู้ให้บริการจนอาจเป็นเหตุให้เกิดความเสียหายแก่ประโยชน์ของประชาชน ธปท. อาจสั่งการให้ระงับการให้บริการรับส่งข้อมูลทั้งหมดหรือบางส่วน รวมถึงห้ามทำธุรกิจใหม่ที่เกี่ยวโยงกับบริการรับส่งข้อมูลดังกล่าว รวมทั้ง ธปท. อาจเปรียบเทียบปรับตามกฎหมายที่เกี่ยวข้อง หรืออาจแจ้งผู้ให้บริการระบบทะเบียน เพื่อพิจารณาเพิกถอนการขึ้นทะเบียนผู้ให้บริการรายดังกล่าวจากระบบทะเบียนฯ

3) เมื่อเกิดปัญหาหรือข้อพิพาทกับลูกค้า[39]

3.1) ผู้ให้บริการต้องรายงานปัญหาหรือเหตุการณ์ผิดปกติที่มีนัยสำคัญ ให้ ธปท.[40] ทราบโดยเร็ว เมื่อเกิดเหตุการณ์หรือเมื่อรับรู้ถึงการเกิดเหตุการณ์ รวมถึงสาเหตุและแนวทางการแก้ไขและป้องกันปัญหามิให้เกิดขึ้นซ้ำอีก และเมื่อมีการวิเคราะห์และกำหนดแนวทางดังกล่าวแล้ว โดยอย่างน้อยต้องครอบคลุมปัญหาหรือเหตุการณ์ดังต่อไปนี้

(1) ปัญหาหรือเหตุการณ์ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบงานหรือการให้บริการรับส่งข้อมูลตามหลักเกณฑ์ฉบับนี้ หรือมีฐานะหรือการดำเนินงานอยู่ในลักษณะอันอาจเป็นเหตุให้เกิดความเสียหายแก่ประโยชน์ของประชาชน

(2) ปัญหาหรือเหตุการณ์ที่นโยบายภายในของผู้ให้บริการกำหนดให้ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด และ/หรือคณะกรรมการที่เกี่ยวข้อง

(3) เหตุการณ์ที่ระบบเทคโนโลยีสารสนเทศของผู้ให้บริการถูกโจมตี หรือถูกขู่โจมตี

3.2) ผู้ให้บริการที่เป็นผู้กระทำผิดหรือเป็นผู้รับผิดชอบปัญหาหรือเหตุการณ์ผิดปกติดังกล่าวต้องดำเนินการดูแล แก้ไข และเยียวยาแก่ลูกค้าอย่างเหมาะสม ตามกฎหมาย หลักเกณฑ์ และแนวปฏิบัติที่กำหนดด้วย[41]

---

[39] กรณีที่ผู้ให้บริการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตาม PDPA เช่น ไม่ส่งข้อมูลตาม consent ของลูกค้าแม้ว่าข้อมูลดังกล่าวได้จัดทำให้อยู่ในรูปแบบ machine readable และมีการจัดทำกลไกการรับส่งข้อมูลแล้ว มีการละเมิดข้อมูลส่วนบุคคลของลูกค้าหรือมีข้อมูลรั่วไหล ลูกค้าสามารถร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตาม PDPA เพื่อพิจารณา ตรวจสอบ และสั่งการตามกฎหมาย รวมถึงสามารถฟ้องเรียกร้องค่าสินไหมทดแทนจากการฝ่าฝืนหรือไม่ปฏิบัติตาม PDPA จนทำให้เกิดความเสียหายต่อลูกค้าในฐานะเจ้าของข้อมูลส่วนบุคคล หรืออาจฟ้องร้องดำเนินคดีทางอาญาหรือขอให้มีการลงโทษทางปกครองหากมีการเปิดเผยข้อมูลโดยไม่ได้รับ consent จากเจ้าของข้อมูลส่วนบุคคลหรือไม่มีฐานทางกฎหมายที่จะกระทำได้

[40] ความมีนัยสำคัญพิจารณาจากระดับความเสี่ยงและผลกระทบ เช่น จำนวนลูกค้าที่ได้รับผลกระทบ ปริมาณข้อมูลที่ได้รับผลกระทบ และความเสียหายที่อาจเกิดขึ้น ทั้งในเชิงความเสียหายด้านการเงิน และชื่อเสียงต่อผู้ที่เกี่ยวข้อง

[41] ธปท. จะร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำแนวปฏิบัติเรื่องการกำหนดความรับผิดในรายละเอียดต่อไป

3.6 กำหนดการดำเนินการตามหลักเกณฑ์

ธปท. พิจารณากำหนดให้ผู้ให้บริการต้องทำกลไกให้แล้วเสร็จและพร้อมให้ลูกค้าใช้สิทธิส่งข้อมูลไปยังผู้ให้บริการรายอื่นได้ตามความพร้อม โดย (1) เริ่มจากข้อมูลเงินฝาก ตามด้วยข้อมูลสินเชื่อและการชำระเงิน เนื่องจากข้อมูลเงินฝากสามารถพัฒนาต่อยอดจากมาตรฐานของบริการ dStatement[42] ที่มีอยู่ในปัจจุบันได้ และ (2) เริ่มจากข้อมูลของลูกค้าประเภทบุคคลธรรมดาก่อน ตามมาด้วยข้อมูลของลูกค้าประเภทนิติบุคคล เพื่อให้ผู้ให้บริการมีเวลาในการพัฒนาระบบพิสูจน์และยืนยันตัวตนนิติบุคคลและพัฒนาระบบรองรับเส้นทางการใช้งาน (journey) สำหรับการส่งข้อมูลนิติบุคคล ซึ่งจะแตกต่างจากของข้อมูลบุคคลธรรมดา ดังนี้

1) ข้อมูลเงินฝากของบุคคลธรรมดา เริ่มให้บริการได้ภายใน 6 ไตรมาสนับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 4 ปี 2569)

2) ข้อมูลสินเชื่อและการชำระเงินของบุคคลธรรมดา เริ่มให้บริการได้ภายใน 7 ไตรมาสนับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 1 ปี 2570)

3) ข้อมูลเงินฝากของนิติบุคคล เริ่มให้บริการได้ภายใน 9 ไตรมาสนับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 3 ปี 2570)

4) ข้อมูลสินเชื่อและการชำระเงินของนิติบุคคล เริ่มให้บริการได้ภายใน 10 ไตรมาสนับตั้งแต่ที่หลักเกณฑ์มีผลบังคับใช้ (คาดว่าภายในไตรมาสที่ 4 ปี 2570)

ทั้งนี้ หลังจากที่หลักเกณฑ์ฉบับนี้มีผลบังคับใช้แล้ว ให้ผู้ให้บริการที่ ณ วันที่หลักเกณฑ์เริ่มมีผลบังคับใช้ยังไม่เข้าข่ายต้องจัดทำกลไก ติดตามจำนวนบัญชี ยอดคงค้าง หรือปริมาณธุรกรรมของตนตามรอบปีบัญชี โดยหากอยู่ในระดับที่เข้าข่ายเป็นผู้ให้บริการที่หลักเกณฑ์กำหนดให้ต้องจัดทำกลไกตามข้อ 3.1 แล้ว ให้ผู้ให้บริการจัดทำกลไกให้ลูกค้าสามารถใช้สิทธิส่งข้อมูลให้แล้วเสร็จและพร้อมให้บริการภายใน 4 ไตรมาสนับจากวันสิ้นรอบปีบัญชีที่ผู้ให้บริการเข้าข่ายต้องจัดทำกลไกตามข้อ 3.1 สำหรับข้อมูลของบุคคลธรรมดา และให้เวลาเพิ่มอีก 3 ไตรมาส สำหรับข้อมูลของนิติบุคคล

อย่างไรก็ตาม กรณีมีเหตุจำเป็นอันสมควรจากปัจจัยที่ผู้ให้บริการไม่สามารถควบคุมได้ ให้ผู้ให้บริการยื่นขอผ่อนผันต่อ ธปท. เป็นรายกรณี โดยแสดงเหตุผล ความจำเป็น และรายละเอียดที่เกี่ยวข้อง ทั้งนี้ ธปท. อาจจะพิจารณาอนุญาตหรือไม่ก็ได้ หรือจะกำหนดเงื่อนไขให้ถือปฏิบัติเพิ่มเติมด้วยก็ได้

---

[42] dStatement คือ การให้บริการรับส่งข้อมูลรายการเคลื่อนไหวบัญชีเงินฝาก (bank statement) ในรูปแบบดิจิทัล ลูกค้าสามารถขอให้ธนาคารที่ตนเองมีบัญชีเงินฝากอยู่ส่งข้อมูล bank statement ไปยังธนาคารแห่งอื่นที่เข้าร่วมโครงการได้โดยตรง โดยการเข้าร่วมโครงการเป็นตามความสมัครใจ และมีธนาคารที่เข้าร่วมโครงการ ณ เดือนธันวาคม 2567 ประกอบด้วย ธพ. และ SFIs จำนวน 10 แห่ง ได้แก่ ธนาคารกรุงเทพ ธนาคารกรุงไทย ธนาคารกรุงศรีอยุธยา ธนาคารกสิกรไทย ธนาคารเกียรตินาคินภัทร ธนาคารไทยพาณิชย์ ธนาคารทหารไทยธนชาต ธนาคารอาคารสงเคราะห์ ธนาคารออมสิน และธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ซึ่งชุดข้อมูลที่ลูกค้าสามารถเรียกได้ในปัจจุบันครอบคลุมเฉพาะบัญชีเงินฝากออมทรัพย์และเป็นการขอข้อมูลแบบเป็นรายครั้ง

4. การดำเนินการภายใต้โครงการ Your Data ในระยะต่อไป

4.1 การดำเนินการในส่วนของข้อมูลในภาคการเงิน

กรอบเวลา	การดำเนินการในส่วนของภาคสถาบันการเงิน (ซึ่งได้ประสานการดำเนินการในส่วนภาคตลาดทุนและภาคประกันภัยให้สอดรับกันด้วย)
วันนี้ – 14 มีนาคม 2568	ธปท. เปิดรับฟังความเห็นจากสาธารณชนต่อแนวทางการกำกับดูแลให้มีกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลที่อยู่กับภาคสถาบันการเงินได้ (ร่างหลักเกณฑ์ฯ)
ภายในไตรมาส 2 ของปี 2568	ธปท. ออกหลักเกณฑ์กำกับดูแลให้มีกลไกที่ลูกค้าสามารถใช้สิทธิส่งข้อมูลที่อยู่กับภาคสถาบันการเงินได้ ให้มีผลใช้บังคับ
ภายในไตรมาส 3 ของปี 2568	ธปท. ประกาศใช้มาตรฐานกลางและแนวปฏิบัติสำหรับการรับส่งข้อมูลชุดแรก โดยอยู่ระหว่างจัดทำร่วมกับผู้ให้บริการและหน่วยงานที่เกี่ยวข้อง
ภายในไตรมาสที่ 4 ปี 2569	ผู้ให้บริการเริ่มให้บริการรับส่งข้อมูลชุดแรก (เงินฝากบุคคลธรรมดา)
ภายในปี 2569	ธปท. ออกหลักเกณฑ์การอนุญาตและการกำกับดูแลการประกอบธุรกิจ Third Party Data Aggregator

4.2 การดำเนินการในส่วนของข้อมูลนอกภาคการเงิน

ธปท. อยู่ระหว่างผลักดันร่วมกับกรมสรรพากร สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) การไฟฟ้านครหลวง การไฟฟ้าส่วนภูมิภาค การประปานครหลวง และการประปาส่วนภูมิภาค พัฒนากลไกให้ประชาชนส่งข้อมูลแบบภาษี และข้อมูลการใช้และการจ่ายชำระค่าไฟฟ้าและน้ำประปาไปยังผู้ให้บริการทางการเงินได้ โดยคาดว่าจะเริ่มให้บริการแก่ลูกค้าได้ในปี 2568

5. ผลลัพธ์ที่คาดหวัง

ธปท. ร่วมกับหน่วยงานที่เกี่ยวข้องผลักดันให้เกิดการพัฒนากลไกให้ลูกค้าใช้สิทธิส่งข้อมูลของตนได้สะดวก ปลอดภัย ไม่ถูกปิดกั้นทางเลือก และใช้งานได้จริง โดยมุ่งหวังให้ประชาชนและผู้ประกอบการสามารถใช้สิทธิส่งข้อมูลของตนที่อยู่ตามที่ต่าง ๆ เพื่อประโยชน์ในการได้รับบริการทางการเงินที่ตอบโจทย์ลูกค้าแต่ละกลุ่มได้ดีขึ้น โดยเฉพาะ (1) การเข้าถึงสินเชื่อในระบบอย่างเหมาะสม โดยเฉพาะรายย่อยที่ไม่มีรายได้ประจำและผู้ประกอบการรายเล็กที่มีความสามารถ แต่มีข้อมูลประวัติทางการเงินกับสถาบันการเงินไม่มากพอ อย่างไรก็ดี ยังมีข้อมูลอื่นอยู่ตามที่ต่าง ๆ และ (2) การบริหารจัดการทางการเงินส่วนบุคคลที่เหมาะกับลูกค้ารายย่อยและผู้ประกอบการรายเล็ก ซึ่งเป็นช่องว่างสำคัญในระบบการเงินไทย

ธปท. คาดหวังว่าเมื่อลูกค้าสามารถใช้สิทธิส่งข้อมูลสำคัญของตนที่มีอยู่ตามที่ต่าง ๆ ได้แล้ว จะเกิดผลลัพธ์ต่อประชาชนและผู้ประกอบการและระบบการเงินในภาพรวม เช่น ผู้ประกอบการรายเล็ก และประชาชนรายย่อยจะสามารถเข้าถึงสินเชื่อที่มีขนาดวงเงิน เงื่อนไข และราคาที่เหมาะกับแต่ละบุคคลได้ดีขึ้น และได้รับบริการ

ที่ช่วยให้แต่ละบุคคลสามารถบริหารจัดการทางการเงินที่เหมาะสมกับวิถีชีวิตและการประกอบอาชีพ รวมถึงประชาชนมีการออมเผื่อฉุกเฉินหรือออมเผื่อเกษียณในสัดส่วนที่มากขึ้น

อย่างไรก็ดี กลไกดังกล่าวจะพัฒนาได้สำเร็จและใช้งานได้จริง จำเป็นต้องอาศัยการผลักดันร่วมกันจากภาคส่วนต่าง ๆ ที่เกี่ยวข้อง ทั้งการเข้ามามีส่วนร่วมจัดทำมาตรฐานกลางและแนวปฏิบัติที่จะใช้งานร่วมกัน และการร่วมให้ความเห็นต่อหลักเกณฑ์ที่เกี่ยวข้อง ธปท. หวังเป็นอย่างยิ่งว่าจะได้รับความเห็นและข้อเสนอแนะของท่านต่อแนวทางกำกับดูแลฉบับนี้ เพื่อที่ ธปท. จะได้นำไปประกอบการจัดทำหลักเกณฑ์ในเรื่องดังกล่าวต่อไป โดยในเบื้องต้นคาดว่าจะสามารถออกหลักเกณฑ์ได้ภายในไตรมาส 2 ปี 2568

ทั้งนี้ ท่านสามารถส่งความเห็นและข้อเสนอแนะต่อแนวทางการกำกับดูแลฉบับนี้มายัง ธปท. ผ่านช่องทางดังต่อไปนี้ ได้ตั้งแต่บัดนี้จนถึงวันที่ 14 มีนาคม 2568

1) ดาวน์โหลดแบบฟอร์มแสดงความคิดเห็นผ่านหน้าเว็บไซต์ ธปท. (www.bot.or.th) และส่งมายังฝ่ายกลยุทธ์สถาบันการเงิน สายนโยบายสถาบันการเงิน ธปท. ทาง Email: opendata-fsd@bot.or.th

2) แสดงความคิดเห็นผ่านหน้าเว็บไซต์ระบบกลางทางกฎหมาย (law.go.th)

เอกสารแนบ

มาตรฐานขั้นต่ำ เรื่อง การรักษาความปลอดภัยของข้อมูล สำหรับผู้ให้บริการที่ให้บริการรับหรือส่งข้อมูลภายใต้หลักเกณฑ์ฉบับนี้

1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management) เพื่อให้ผู้ให้บริการมีทะเบียนรายการทรัพย์สินด้าน IT ที่เกี่ยวข้องกับการให้บริการอย่างครบถ้วน และสามารถใช้ทะเบียนทรัพย์สินเหล่านั้นในการกำหนดแนวทางควบคุมทรัพย์สินดังกล่าวอย่างเหมาะสมตามระดับความเสี่ยง

2) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security) เพื่อให้ผู้ให้บริการมีการจัดการข้อมูลที่ปลอดภัย โดยมีวิธีการจัดการข้อมูลที่สอดคล้องตามการจัดชั้นความลับข้อมูล (information classification) และครอบคลุมตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การจัดเก็บ การใช้งาน และการทำลายข้อมูล

3) การควบคุมการเข้าถึง (access control) เพื่อให้ผู้ให้บริการมีการป้องกันการเข้าถึงระบบงานและข้อมูลของลูกค้าโดยไม่ได้รับอนุญาต โดยอย่างน้อยต้องมีการพิสูจน์ตัวตนแบบ multi-factor authentication ครอบคลุมบัญชีผู้ใช้งานที่มีสิทธิสูง และบัญชีผู้ใช้งาน (users) ของผู้ให้บริการที่สามารถเข้าถึงข้อมูลของลูกค้าผ่านเครือข่ายสาธารณะ (Internet) ได้

4) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security) เพื่อให้ผู้ให้บริการมีโครงสร้างระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย ครอบคลุมการออกแบบ และบริหารจัดการระบบเครือข่ายสื่อสารให้มีความปลอดภัย สอดคล้องตามมาตรฐานสากลอย่างสม่ำเสมอ และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ โดยเฉพาะในจุดที่มีการเชื่อมต่อกับ Internet

5) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) เพื่อให้สามารถป้องกันภัยจากโปรแกรมไม่ประสงค์ดี (malware) หรือการโจมตีด้วยรูปแบบต่าง ๆ รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ

6) การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening) เพื่อให้ระบบงานที่รองรับการให้บริการมีการตั้งค่าความปลอดภัยที่สอดคล้องกับมาตรฐานสากล โดยผู้ให้บริการต้องมีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และตั้งค่าการรักษาความมั่นคงปลอดภัยระบบงานให้เป็นไปตามมาตรฐานที่กำหนด รวมทั้งสอบทานการตั้งค่าให้เป็นไปตามที่กำหนดอย่างสม่ำเสมอ

7) การสำรองข้อมูล (Data backup) เพื่อให้มั่นใจว่าผู้ให้บริการมีการดูแลข้อมูลของลูกค้าให้มีความพร้อมใช้งานกรณีข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการสำรองข้อมูลให้สอดคล้อง

กับความสำคัญของข้อมูล รวมทั้งจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสำรองให้สอดคล้องตามระดับชั้นความลับของข้อมูล นอกจากนี้ ต้องทดสอบความพร้อมใช้ของข้อมูลสำรองอย่างสม่ำเสมอ

8) การบริหารจัดการการเปลี่ยนแปลง (change management) เพื่อให้ผู้ให้บริการมีการควบคุมการเปลี่ยนแปลงระบบงานเป็นไปอย่างรัดกุมปลอดภัย และป้องกันการเปลี่ยนแปลงแก้ไขระบบงานโดยไม่ได้รับอนุญาต ครอบคลุมกระบวนการที่สำคัญ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration) การติดตั้ง patch

9) การบริหารจัดการ security patch เพื่อให้ระบบงานที่ให้บริการมีกระบวนการปิดช่องโหว่อย่างรัดกุมและเหมาะสมทันการณ์ ลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องจัดให้มีกระบวนการบริหารจัดการ security patch ให้เหมาะสมตามระดับความเสี่ยง ให้ครอบคลุมทุกระบบงานและอุปกรณ์

10) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) เพื่อให้ผู้ให้บริการสามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการหรือเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์

11) การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing) เพื่อให้ระบบงานของผู้ให้บริการสามารถป้องกันภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยมีการประเมินช่องโหว่ (vulnerability assessment) สำหรับระบบงานสำคัญอย่างน้อยปีละครั้ง รวมทั้งมีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่เป็นอิสระ ซึ่งอย่างน้อยครอบคลุมระบบงานที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (Internet facing)

12) การจัดหาและการพัฒนาระบบ (system acquisition and development) โดยผู้ให้บริการมีกระบวนการจัดหาและการพัฒนาระบบงานที่มีการควบคุมการรักษาความมั่นคงปลอดภัยอย่างรัดกุมและเป็นไปตามมาตรฐานสากล ดังนี้

12.1) การจัดหาระบบ ผู้ให้บริการต้องกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ เช่น ความน่าเชื่อถือของระบบ บุคคลภายนอกที่ให้บริการที่ได้รับการรับรองตามมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการ มีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานที่ผู้ให้บริการกำหนดและสอดคล้องตามมาตรฐานสากล รวมทั้งสามารถตอบสนองต่อความต้องการในการดำเนินการได้

12.2) การพัฒนาระบบ ผู้ให้บริการต้องออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ พร้อมใช้งาน และมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานที่ผู้ให้บริการกำหนดและสอดคล้องตามมาตรฐานสากล

13) การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) เพื่อให้ผู้ให้บริการมีแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างรัดกุม มีการรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง บนพื้นฐานที่ผู้ให้บริการยังคงไว้ซึ่งความรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการลูกค้า โดยครอบคลุมตั้งแต่การประเมินความเสี่ยง การคัดเลือกบุคคลภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่อง และการยกเลิก หรือสิ้นสุดสัญญาหรือข้อตกลง

14) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของลูกค้าย้อนหลัง (audit trail) และการจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) โดยผู้ให้บริการต้องดำเนินการดังนี้

14.1) จัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ตรวจสอบร่องรอยการเข้าถึง และการใช้งานระบบหรือข้อมูลที่รองรับการให้บริการ รวมทั้งสามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนดด้วย

14.2) จัดเก็บ audit trail ในลักษณะรายธุรกรรมและมีรายละเอียดอย่างน้อย ประกอบด้วย

(1) ข้อมูลการให้ consent และ authorization สำหรับการรับส่งข้อมูล

(2) ข้อมูลการแก้ไขและการเพิกถอน consent และ authorization และ

(3) ข้อมูลการรับส่ง และการใช้ข้อมูลของผู้ให้บริการที่รับข้อมูล โดยกำหนดให้จัดเก็บ audit trail เป็นเวลา 10 ปี[43]

[43] กำหนดระยะเวลาจัดเก็บเป็นเวลา 10 ปี เพื่อให้สอดคล้องกับอายุความของการใช้สิทธิเรียกร้องค่าเสียหายในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลตามที่กำหนดในหมวด 6 เรื่องความรับผิดทางแพ่ง ของ PDPA ทั้งนี้ การกำหนดระยะเวลาการจัดเก็บ audit trail ตามอายุความที่กำหนดในกฎหมายที่เกี่ยวข้องนั้นสอดคล้องกับแนวทางของหลายประเทศ เช่น สหราชอาณาจักร ออสเตรเลีย บราซิล ทั้งนี้ ผู้ให้บริการภายใต้การกำกับของ ธปท. ในปัจจุบันบางส่วนจัดเก็บข้อมูลเป็นระยะเวลา 10 ปี เพื่อให้ไปตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินอยู่แล้ว