สรุปคำถาม คำชี้แจง ภาคการเงิน

การสัมมนาแนะนำกฎหมายคุ้มครองข้อมูลส่วนบุคคล วันที่ 10 ตุลาคม 2562

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
๑.	การตีความบทลงโทษทางอาญาตามมาตรา ๗๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตีความอย่างไร มาตรา ๗๙ บัญญัติว่า “ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ ...” ข้อความตามมาตรา ๗๙ ที่กำหนดว่า “อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖” ขยายความไปถึงการใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๗ ด้วยหรือไม่ หรือขยายความเฉพาะการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามมาตรา ๒๘ เท่านั้น	คำถามนี้เป็นคำถามที่อยู่ในกระบวนการของชั้นศาลแล้ว แต่มีข้อแนะนำว่าควรที่จะมีการกำหนด guideline ให้เป็นไปในทิศทางเดียวกันเพื่อป้องกันไม่ให้มีกรณีไปถึงชั้นศาลหรือหากมีกรณีที่จะต้องไปถึงชั้นศาลก็สามารถที่จะมีคำอธิบายที่ตรงกันได้ในเรื่องนี้	
๒	กิจกรรมดังนี้ใช้ฐาน Legitimate Interest ได้หรือไม่ • Upselling (วิเคราะห์ข้อมูล/ใช้ข้อมูลเพื่อเสนอผลิตภัณฑ์ประเภทเดียวกับที่ลูกค้ามีอยู่) • Cross selling (วิเคราะห์ข้อมูล/ใช้ข้อมูลเพื่อเสนอผลิตภัณฑ์อื่นของธนาคาร) • สิทธิประโยชน์พิเศษโดยไม่มีวัตถุประสงค์ทางการตลาด อาทิเช่น กรณีที่ลูกค้าซื้อกองทุนแล้วกองทุนครบอายุ ก็อาจจะมีกองทุนมารับต่อจะแจ้งได้หรือไม่ว่ากองทุนครบอายุแล้ว หรือกรณีการส่ง Birthday gift ไปให้เนื่องจากใกล้วันเกิดแล้ว หรือการเตือนการจ่ายค่าน้ำค่าไฟ ซึ่งล้วนเป็นประโยชน์ของ Data Subject ทั้งสิ้น	เมื่อกล่าวถึง Legitimate Interest เป็นความจำเป็นเป็นส่วนได้เสียของธนาคารที่ธนาคารจะต้องทำได้ คำถามว่าจะเสนอขายผลิตภัณฑ์นั้นขึ้นอยู่กับบริบทของเรื่องนั้นๆ ว่ามีความจำเป็นอย่างไร สามารถอธิบายได้ว่ามีความจำเป็น ซึ่งกรณีที่ลูกค้าซื้อกองทุนแล้วกองทุนครบอายุก็อาจจะมีกองทุนมารับต่อ ถ้าเป็นแบบนี้มีความเป็นไปได้ที่จะอธิบายได้	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
๓.	Partner ใช้สิทธิตาม Consent ของ Partner เปิดเผยข้อมูลมายังธนาคาร ธนาคารไม่ต้องทำตามมาตรา ๒๕ แล้วใช่หรือไม่ คือในระบบของธนาคารจะมีการรับส่งข้อมูลระหว่าง Partner หรือในเครือธนาคารระหว่างกัน การที่ Consent บน Data Controller คนแรกที่เป็น Partner มีสิทธิเปิดเผยมาให้เพียงพอแล้วหรือไม่ จะต้องกลับไปขอ Consent Data Subject อีกครั้งหนึ่งหรือไม่	ตามหลักการคือว่ากรณีที่จะได้ข้อมูลนั้นต้องมีฐานในการประมวลผล ซึ่ง Consent ก็เป็นหนึ่งในฐานนั้น การได้ข้อมูลจากแหล่งอื่นโดยหลักแล้วต้องไปขอ Consent ในเมื่อต้นทางมีฐานมาแล้วแล้วส่งมาให้ก็ไม่ต้องไปทำซ้ำอีก ยกตัวอย่างเช่น ถ้าเป็นเรื่อง marketing ไปซื้อ lead รายชื่อมา ถ้าต้องไปขอ Consent ตามรายชื่อนั้นใหม่ อย่างนี้ก็เหมือนต้องทำงานอีกครั้งหนึ่ง ไม่มีความจำเป็นที่จะต้องซื้อ lead มา เพราะฉะนั้น คือต้องเป็นเรื่องที่เสร็จตั้งแต่ต้นทางมาแล้วไม่ควรที่จะต้องมาทำใหม่	
๔.	ถ้า Data Subject ให้ Consent กับ Data Controller A ไปแล้ว Data Controller A ก็เปิดไปให้ Data Controller B จะทราบได้อย่างไรว่าข้อมูลนี้จะถูกเปิดไปที่ผู้ใดบ้าง ถ้าต้องการที่จะไปขอใช้สิทธิ	กรณีนี้เรียกว่า Data sharing คือจะ sharing กันไปเรื่อยๆ ทุกคนจะเป็น Controller ร่วมกัน จะเป็นความรับผิดชอบร่วมกัน ในทางปฏิบัติเพื่อไม่ให้มีปัญหาต้นทางต้องทำให้เสร็จหมดเลยทุกอย่าง เพราะฉะนั้นคำถามจะไม่ทราบเลยว่าจะไป sharing ให้ใครมันจะไม่เกิดขึ้น คำถามว่าจะไม่รู้ว่าจะไปแจ้งลบที่ไหนมันก็จะไม่เกิดขึ้น	
๕.	กรณีแรก ถ้าธนาคารมีการเก็บประวัติลูกค้าเก่าๆ ที่เป็นหนี้สินกับธนาคาร ธนาคารแห่งประเทศไทยจะดำเนินการอย่างไรได้บ้าง เพื่อให้ธนาคารทราบว่าควรที่จะมีการบริหารความเสี่ยงภายในกรณีที่สอง ในการทำการค้านั้นมีการสนับสนุนให้ผู้ประกอบการไปต่างประเทศ ถ้ามีการซื้อข้อมูลจากองค์กรติดตามของต่างประเทศที่ทำถูกต้องตามกฎหมายของประเทศนั้นแล้ว ต่อมามีการขายข้อมูลที่ซื้อมานั้นให้กับผู้ประกอบการซึ่งการดำเนินการทำถูกต้องตามกฎหมายก่อนที่	กรณีแรก เป็นเรื่องในทางปฏิบัติ ซึ่งธนาคารแห่งประเทศไทยสามารถที่จะช่วยได้ กรณีที่สอง ขอทำความเข้าใจให้ทราบว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ไม่ได้มีส่วนทำให้ต้องเปิดอะไรหรือปิดอะไร การจะเปิดหรือปิดอะไรเป็นไปตามกฎหมายของท่านถ้าท่านมีกฎหมาย หรือถ้ามีสัญญาก็เป็นไปตามสัญญา เพียงแต่ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคล	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ใช้บังคับ เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ใช้บังคับแล้ว ยังสามารถดำเนินการต่อไปได้หรือไม่		
๖.	ถ้าจะ design ในเรื่องของการ access ของข้อมูล มีการควบคุมการใช้สิทธิการ access เข้ามา รวมถึงการลบข้อมูล แนวคิดของการ design ลักษณะนี้ตอบโจทก์ของพระราชบัญญัติฯ นี้แล้วหรือไม่ ซึ่งถ้าทำได้ การลบข้อมูลถ้าลบไปเลยจากฐานข้อมูลขององค์กรทำได้ยากและมีประเด็นปัญหาที่ตามมา แต่ถ้าหากเป็นการลบโดยลบการอ้างอิงตัวบุคคลได้จะตอบโจทก์ในพระราชบัญญัติฯ นี้ได้หรือไม่	จากคำถามนั้นตอบโจทก์หลายอย่างแต่ว่าไม่จำเป็นต้องเป็นแบบนี้เท่านั้น มันอาจจะเป็นแบบอื่นก็ได้ การลบซึ่งเป็นเรื่องในทางปฏิบัติ กฎหมายไม่ได้ไปกำหนดว่าต้องเป็นอย่างนี้ไม่เป็นอย่างอื่นแล้วแต่ว่าจะสะดวกอย่างอื่นก็ทำได้เหมือนกัน ในทางปฏิบัติต้องแน่ใจว่าที่ทำนะทำได้ แต่ก็มีมาตรฐานเพิ่มเติมอยู่ดี ก็ยังต้องมีมาตรการกำกับอยู่	
๗.	กรณีที่ลูกค้ามาปิดบัญชี เมื่อพ้นเวลาที่กฎหมายกำหนดแล้ว ๑๐ ปี ในการที่จะจัดเก็บ ธนาคารสามารถที่จะเก็บข้อมูลการทำธุรกรรมที่ลูกค้ามาทำกับธนาคารนี้ได้ต่อหรือไม่	อธิบายได้หรือไม่ว่ามีความจำเป็นจะต้องทำอย่างนั้น ข้อมูลที่จัดเก็บมีประโยชน์ต่อเราอย่างไร มีมาตรการที่จะคุ้มครองข้อมูลอย่างไร	
๘.	ลูกค้าฝากเงินไว้และมาถอนเงินแล้วมีการปิดบัญชีแล้ว ต่อมาผ่านไป ๒๐ ปี ลูกค้าก็กลับมาแล้วแจ้งว่าไม่เคยถอน แต่ว่าข้อมูลนี้มันขาดไปแล้ว ธนาคารจะเก็บข้อมูลนี้ไว้ได้หรือไม่	ถ้าอธิบายได้ว่ามีความจำเป็น ซึ่งต้องอธิบายว่ามีความจำเป็นอย่างไร	
๙.	ข้อมูลที่เก็บคือข้อมูลสุขภาพ ประวัติการรักษาจากโรงพยาบาลว่ามาจากไหน ว่าถ้าลูกค้ายังอยู่กับเรา เราเก็บข้อมูลไว้ได้ แต่กรณีที่ลูกค้าเกิดยกเลิกกรมธรรม์เราอาจจะต้องเก็บข้อมูลเอาไว้เผื่อลูกค้ากลับมาอีก อาจจะต้องพึ่งพา	ได้ครับ หลักๆ คือเราต้องรับไปทำต่อ ซึ่งมีความสำคัญถ้ามีการกำหนดระยะเวลาออกมาทุกคนก็จะได้ปฏิบัติตามนั้น	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	regulator ของเราในการออกกฎ อาจจะต้องฝากทางสำนักงานฯ ได้หรือไม่		
๑๐.	ความยินยอมตามพระราชบัญญัติฯ มีทั้งกรณีที่เป็น Personal Data และกรณีที่เป็น Sensitive Data ถ้าเป็นความยินยอมของ Personal Data ความยินยอมนั้นจะเป็นประมาณไหน	มาตรา ๑๙ กำหนดว่าโดยชัดแจ้ง มีตัวอย่างในสถานการณ์ปกติทั่วไปในตอนนี้ มาตรฐานสากลจะใช้คำตอบว่า yes หรือ no แต่ว่าหลายสถานการณ์ไม่ได้ตายตัวมันขึ้นอยู่กับแต่ละบริบท เป็นเราที่ควรจะต้องอธิบายออกมาว่าสถานการณ์แบบนี้ควรจะใช้ Consent แบบไหน เพื่อให้มีความเข้าใจที่ตรงกัน	
๑๑.	ความต่างระหว่างความยินยอมของ Personal Data กับ Sensitive Data ต้องต่างกันขนาดไหน	ควรจะทำความเข้าใจตามสถานการณ์ของเรื่องมากกว่า เช่น ถ้าเป็นแบบฟอร์มทางการเงินเปิดบัญชีจะเป็นอย่างนี้ ถ้าเป็นเรื่องนี้จะเป็นอย่างนี้ ทุกเรื่องขึ้นอยู่กับสถานการณ์แล้วอธิบายว่าควรจะเป็นอย่างไร	
๑๒.	ไม่มีกฎหมายกำหนดว่าให้เก็บได้แต่เก็บเพื่อโอกาสในอนาคตหากมีคดีความเกิดขึ้นเพื่อใช้ในการต่อสู้คดี จะตีความไปถึงว่าเป็นอายุความในการต่อสู้คดีได้หรือไม่	เรื่องนี้น่าจะแก้ไขได้ด้วยธนาคารแห่งประเทศไทย ซึ่งสามารถช่วยได้	
๑๓.	ข้อมูลที่จะให้ลูกค้าใช้สิทธิ Access/Port จะมีเฉพาะข้อมูล Profile และข้อมูลธุรกรรมของลูกค้าเท่านั้น โดยไม่รวมถึงข้อมูลการทำแบบจำลองเครดิตหรือข้อมูลที่ธนาคารวิเคราะห์ขึ้นได้หรือไม่ กล่าวคือ กฎหมายกำหนดว่าลูกค้าเจ้าของข้อมูลมีสิทธิขอเข้าถึงขอใช้สิทธิของข้อมูลส่วนบุคคลที่เกี่ยวกับตน ข้อมูลส่วนบุคคลที่เกี่ยวกับตนคือข้อมูลส่วนไหนบ้าง ถ้าข้อมูล Profile ของลูกค้าก็ให้เข้าถึงได้ แต่ถ้าเป็นข้อมูล	จะต้องมีคำอธิบายที่ทำให้คนทั่วไปเข้าใจตรงกันว่าจะเป็นอย่างไร	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	ที่เกี่ยวกับลูกค้า เช่น เป็นข้อมูลที่ธนาคารวิเคราะห์ขึ้น กรณีนี้จะตีความไปถึงด้วยหรือไม่		
๑๔	ถ้ามี application ที่ต้องระบุข้อมูล Personal Data ส่วนหนึ่ง และที่เป็น Sensitive Data application นี้ลูกค้าทำขึ้นเพื่อจะทำสัญญาด้วย ซึ่งจะเป็นไปตามมาตรา ๒๔ (๓) ที่ไม่ต้องทำ Consent แล้วในส่วนที่เป็นข้อมูล Sensitive Data ที่เป็นเรื่องข้อมูลสุขภาพที่มีอยู่ใน application ด้วย ควรที่จะต้องทำ Consent ตามมาตรา ๒๖ หรือไม่ และถ้าต้องทำ application นี้ต้องมีการเพิ่ม wording เข้าไปเพื่อให้เห็นว่ามี Consent อยู่ใน application หรือไม่ และหากในอนาคตถ้าลูกค้าขอเพิกถอน Consent จะอ้างว่ายังมีสัญญาประกันภัยอยู่จะไม่ให้เพิกถอนได้หรือไม่	ต้องทำเพราะกฎหมายบอกให้ทำกฎหมายบอกให้ต้องขอความยินยอม กรณี Sensitive Data ถ้าหลุดไปเจ้าตัวจะถูกเลือกปฏิบัติได้ซึ่งมีความสำคัญมาก เพราะฉะนั้น เจตนาก็เพื่อให้เจ้าตัวรู้ว่าข้อมูล Sensitive จะถูกเก็บ จึงจำเป็นที่จะต้องแสดงให้เห็นชัดว่ากำลังเก็บข้อมูล Sensitive Data อยู่ ถ้าลูกค้าไม่ให้ใช้ ต้องอธิบายว่ามีความจำเป็นอย่างไร	
๑๕	ในกรณีที่สถาบันการเงินจะต้องมีการนำชื่อไปตรวจสอบ ซึ่งฐานข้อมูลอาจจะได้จาก ปปง. เช่น ลูกค้าอาจจะเป็นชื่อ ก แต่อาจจะไปพบว่ามีความสัมพันธ์กับ ข หรือ ค ซึ่ง ข หรือ ค ไม่ใช่ลูกค้าของสถาบันการเงิน อาจจะเป็นนักการเมืองหรืออาจจะมีการต้องหาคดีต่างๆ เช่นนี้ ต้องส่งหนังสือแจ้งให้กับ third party ว่าได้พบชื่อในฐานข้อมูลอีกฐานหนึ่งหรือไม่	ถ้าเป็นส่วนหนึ่งของการตรวจสอบการกระทำความผิดทางการเงินซึ่งอยู่ใน scope ที่กฎหมายให้ต้องทำ ซึ่งต้องอธิบายออกมา ต้องไปพูดคุยกันว่าควรจะเป็นยังไง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ไม่ได้กำหนดให้เปิดหรือปิดอะไร จึงเห็นว่าไม่ได้เป็นการขัดแต่อย่างใด	
๑๖	การขอ Consent เก็บ Sensitive Data ต้องขอใหม่ทุกครั้งหรือไม่ และถ้าเป็นการเก็บ	ถ้ามีการเก็บใหม่โดยหลักต้องขอใหม่ เป็นคำถามที่ดี ขอรับไว้เพื่อตรวจสอบว่า signature เป็น Sensitive Data หรือไม่	ขอรับประเด็นไว้เพื่อตรวจสอบ

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	signature จะเป็น Sensitive หรือไม่ ต้องขอ Consent หรือไม่		
๑๗	ตามมาตรา ๓๑ การโอนข้อมูลโดยอัตโนมัติ ซึ่งตอนนี้ธนาคารจะโอนข้อมูลในโครงการ MDID จะสามารถส่งข้อมูลระหว่างธนาคารของลูกค้าที่สมัครโครงการ จะเข้ากรณีตามมาตรา ๓๑ หรือไม่	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ไม่ได้กำหนดให้เปิดหรือปิดอะไร จะเปิดหรือจะปิดอะไรต้องกำหนดเอง ซึ่งต้องทำให้ได้มาตรฐานคุ้มครองข้อมูลส่วนบุคคล	
๑๘	แนวทางในการทำงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกับ regulator ต่างๆ เช่น ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) จะทำงานร่วมกันอย่างไรในการที่จะช่วยผลักดันส่งเสริมเรื่องนี้ให้เกิดความชัดเจน	คงต้องมีการพูดคุยทำความเข้าใจกัน และที่สำคัญสำนักงานฯ มีความตั้งใจที่จะเข้าไปดูหน่วยงานรัฐเพื่อให้หน่วยงานรัฐสามารถมีการทำงานเรื่องนี้ขึ้นมา และที่สำคัญคือควรจะมี guideline เพื่ออธิบายออกมาให้เห็นอย่างชัดเจน	
๑๙	นโยบายของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้นมีนโยบายจะส่งผู้ตรวจเข้าตรวจสถาบันการเงินเหมือนอย่างเช่นธนาคารแห่งประเทศไทยหรือไม่	โดยหลักทั่วไป regulator คือคนตรวจ แต่สิ่งแรกเลยคือต้องทำให้ทุกคนรู้และเข้าใจว่าจะต้องทำอย่างไร	
๒๐	ถ้าเกิดจะใช้กล้องในการบันทึกในพื้นที่ของเราเองแต่ว่าอาจจะทำข้อมูลใบหน้าลูกค้าและคนที่มาด้วยที่ไม่ใช่ลูกค้าซึ่งอาจเป็นการฝ่าฝืนหรือไม่ ถ้าจะเก็บไว้เพื่อวัตถุประสงค์อื่นที่ไม่ใช่ security อาจจะเอาไว้ใช้ในธุรกิจของธนาคารแต่ไปติดบุคคลอื่นที่ไม่ใช่ลูกค้า	การจะเก็บหรือไม่เก็บพระราชบัญญัติฯ นี้ไม่ได้กำหนดว่าจะเก็บหรือไม่เก็บอะไร แต่กำหนดว่าถ้าจะเก็บให้อธิบายว่าเก็บตามฐานไหนและเก็บอย่างไร มีมาตรการคุ้มครองอย่างไร ตัวอย่างที่ยกมาเป็นตัวอย่างที่ดีมาก พอมีการเก็บหน้าก็จะเป็น Sensitive Data จะอัตโนมัติเลยว่ามีความเสี่ยงสูง ต้องทำการประเมินความเสี่ยง ซึ่งในอนาคตจะต้องมีอย่างแน่นอน ที่เรียกว่า DPIA หรือ Data Protection Impact Assessment	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
๒๑	ถ้าเกิดเจอข้อผิดพลาดหรือข้อที่ดูเหมือนจะไม่สอดคล้องกับกฎหมายที่กำหนดเอาไว้ จะดำเนินการอย่างไรบ้าง	ถ้าเป็นความผิดพลาดแบบไม่ตั้งใจ มี process รองรับหรือไม่ ถ้าไม่มีรองรับอาจจะมีปัญหา อาจจะเป็นความตั้งใจที่จะไม่มี process ได้ แต่ถ้ามี process แล้วมีการให้ความเห็นไม่ตรงกัน อย่างนี้จะเป็นเรื่องปกติถือว่าไม่ได้มีปัญหาอะไรแค่ความเห็นไม่ตรงกันซึ่งมีการให้เหตุผลไว้เป็นปกติที่เกิดขึ้นอยู่แล้ว	
๒๒	การขอ Consent กฎหมายกำหนดว่าจะต้องง่ายเข้ากันกับการให้ Consent คำว่า ง่ายเข้ากันนั้นตีความอย่างไร เช่น ให้ Consent channel นี้ ถ้าจะถอนก็ต้องถอนจาก channel เดิมที่ให้ Consent	จากตัวอย่างก็อยู่ในความหมายด้วยเหมือนกัน หรืออย่างเช่น การขอ Consent ด้วยวิธีการกด App แต่พอจะถอนไปใช้วิธีการที่ยากกว่าเช่นจะต้องเข้าไปที่ office ซึ่งอย่าให้เป็นประเด็นเลย หลักๆ ก็คือเท่ากันดีที่สุด เท่ากันจะอธิบายง่าย มาอย่างนี้ออกอย่างนี้	
๒๓	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ กำหนดว่าถ้ามีกฎหมายอื่นที่คุ้มครองข้อมูลส่วนบุคคลอยู่แล้วให้ใช้กฎหมายอื่น ซึ่งในเรื่องเกี่ยวกับ Consent ที่มีการกำหนดไว้ใน market conduct ของธนาคารแห่งประเทศไทย ซึ่งเมื่อดูพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ แล้วมีการกำหนดว่าให้ไปใช้ของธนาคารแห่งประเทศไทย จะมีการพูดคุยในกรณีนี้กันหรือไม่	ควรมีการพูดคุยกันแน่นอน ซึ่งขอรับประเด็นนี้ไว้	สำนักงานฯ จะรับประเด็นไว้
๒๔	ข้อมูลของผู้เสียชีวิตมีความหมายอย่างไร และสามารถที่จะปฏิบัติกับข้อมูลของผู้ตายได้ขนาดไหนเพราะว่าข้อมูลของผู้ตายไม่ได้อยู่ในนิยามของข้อมูลส่วนบุคคล ถ้าเกิดลูกค้าบัญชีเงินฝากเสียชีวิตไปแล้ว ธนาคารสามารถใช้ข้อมูลของลูกค้าที่เสียชีวิตได้หรือไม่	ขออธิบายว่าถ้ามีคนตายจะไม่เข้าความหมายข้อมูลส่วนบุคคล จะไม่มีประเด็นเกี่ยวกับเรื่องข้อมูลส่วนบุคคลแล้ว	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
๒๕	ถ้ากฎหมายอื่นๆ ขัดกับที่ PDPA วางไว้ อย่างเช่น ประกาศของธนาคารแห่งประเทศไทยที่เป็น market conduct ซึ่งถ้าอ่านประกาศเสมือนว่าใช้ Consent ได้อย่างเดียว แปลว่าถ้าฐานอื่นๆ ที่ไม่ใช่ Consent ตาม PDPA ใช้ได้หรือไม่ เพราะมาตรา ๓ กำหนดว่าถ้ามีกฎหมายอื่นเป็นการเฉพาะอยู่แล้วจะใช้ PDPA เป็นการเพิ่มเติมในเฉพาะบางเรื่อง	การที่เราพูดว่า Consent อย่างเดียว Consent นั้น คือ Consent แบบ PDPA เพราะ Consent ของ market conduct ไม่ได้มีการนิยามไว้เหมือนกับ PDPA Consent ของธนาคารแห่งประเทศไทยจึงไม่ได้ใช้ความหมายนี้อยู่แล้ว กฎหมายสองฉบับโดยหลักแล้วจะไม่ขัดกันคือเราจะไม่ตีความให้มันขัดกัน เพราะฉะนั้นกรณีนี้มันไม่ขัดกัน ซึ่งถ้าจะต้องแก้ไขให้มีความชัดเจนตรงกัน สำนักงานฯ จะรับไปพูดคุยกับธนาคารแห่งประเทศไทย	สำนักงานฯ จะรับประเด็นไว้
๒๖	สาขาในต่างประเทศ (เช่น ใน CLMV) อยู่ภายใต้ PDPA หรือไม่ (บริษัทแม่ไม่มีการส่งข้อมูลไปยังสาขาต่างประเทศแต่อาจมีกรณีที่สาขาส่งข้อมูลกลับมาเพื่อการบริหารจัดการภายในองค์กร)	ในกรณีนี้สาขาไม่ใช่ประเด็น ประเด็นคือตัว Data ว่า Data อยู่หรือไม่ ถ้าเป็น Data ของประเทศไทยก็อยู่ภายใต้กฎหมายนี้	
๒๗	ข้อยกเว้นตามมาตรา ๒๘ (๑) รวมถึงกฎหมายต่างประเทศที่มีผลใช้บังคับกับธนาคาร เช่น GDPR ด้วยหรือไม่	ถ้าเป็นธนาคารต่างชาติต้องทำตาม GDPR อยู่แล้ว เพราะฉะนั้น เราจะอ้างการทำตาม GDPR เพื่อจะส่งข้อมูลไปต่างประเทศได้หรือไม่ ซึ่งมีทางออกหลายทาง เพราะ GDPR ถือว่าเป็นกลุ่มประเทศที่มีความคุ้มครองดีอยู่แล้วสามารถทำได้หลายอย่าง โดยหลักแล้วถ้ามีการคุ้มครองข้อมูลส่วนบุคคลก็สามารถส่งได้	
๒๘	ถ้าเป็นกรณีที่มีบริษัทแม่อยู่ที่ต่างประเทศแล้วในฐานะที่เป็นบริษัทลูกจะต้องปฏิบัติตามกฎหมายต่างประเทศที่ทำให้เราต้องส่งข้อมูลส่วนบุคคลของลูกค้าไปต่างประเทศ ถ้าเป็นเพียงมีหน้าที่ที่จะต้องส่งข้อมูล หน้าที่ที่จะต้องรายงาน แต่ยังไม่ถึงขั้นที่จะใช้สิทธิ ซึ่งบริษัทแม่อยู่ในประเทศที่	การอ้างการปฏิบัติตามกฎหมาย ต้องเป็นการใช้สิทธิตามกฎหมาย แต่ตามตัวอย่างที่ยกมานั้นยังไม่ใช่ แต่ถ้ามันเข้าสู่กระบวนการการใช้สิทธิตามกฎหมายที่มีการฟ้องคดีเรียกพยานหรือข้อมูลไปเช่นนี้อันนี้ถึงจะใช่ แต่ว่าจากตัวอย่างจะขอไปตรวจสอบให้	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	ไม่ได้มีความคุ้มครองที่เพียงพอ เช่นนี้ จะเข้าข้อยกเว้นตามมาตรา ๒๘ (๑) หรือไม่		
๒๙	กรณีถอน Consent ข้อจำกัดสิทธิโดยมีสัญญาที่ให้ประโยชน์แก่ลูกค้าหมายถึงอะไร เหตุใดไม่ใช้ฐาน Contract ต่อไป	อาจจะยกเป็นตัวอย่างเช่น ถ้าคุณให้ข้อมูลกับทางเราและสมัครสมาชิก เราให้ส่วนลดเท่านี้ แต่พอคุณไม่ให้ข้อมูลเราก็จะไม่ให้สิทธิส่วนลด อย่างนี้มีเงื่อนไขตรงนี้ได้ แต่เงื่อนไขตรงนี้จะต้องไม่มากระทบสัญญาหลัก	
๓๐	ข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะมีข้อมูลของลูกค้าและรวมอยู่กับข้อมูลของลูกค้ารายอื่นด้วย ถ้าเกิดลูกค้ารายหนึ่งจะมาขอใช้สิทธิที่จะลบข้อมูลซึ่งทางไอทีอาจจะทำไม่ได้ เช่นนี้ จะมีวิธีการหรือทางออกอย่างไรได้บ้าง	เป็นเรื่องในทางปฏิบัติ ถ้าจะต้องลบแล้วจะลบอย่างไร ซึ่งต้องมีวิธีการที่สามารถทำได้	
๓๑	ถ้าเกิดว่าจะเก็บข้อมูลจาก CCTV มีความจำเป็นต้องติดป้ายแจ้งทุกๆ ที่ที่มีกล้องหรือไม่ ถ้าเกิดมีคนมาขอข้อมูลในกรณีนี้คือข้อมูล CCTV และถ้ามีค่าใช้จ่ายในการนำข้อมูล CCTV นั้นออกมาสามารถเรียกเก็บค่าใช้จ่ายได้หรือไม่	ค่าใช้จ่ายเรียกเก็บได้แต่ครั้งแรกไม่ควรจะเก็บ ต่อมาก็คือว่าควรจะติดทุกที่หรือไม่ ทุกที่ในความหมายนี้คือทุกกล้อง คือจริงๆ แล้วควรจะต้องช่วยกันอธิบายว่าถ้าเป็นกรณีนี้จะเป็นอย่างไร ควรจะเห็นเป็นห้องหรือควรจะเห็นเป็นสถานที่ ซึ่งควรจะช่วยกันเขียนออกมาบอกให้มันชัดเจน	
๓๒	มาตรา ๒๑ ที่กำหนดว่าผู้ควบคุมข้อมูลต้องเก็บใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้ ถ้ากรณีมีการเปลี่ยนวัตถุประสงค์ใหม่ก็จะต้องมีการแจ้งให้กับเจ้าของข้อมูลและได้รับความยินยอม ถ้าธนาคารแห่งประเทศไทยได้รับข้อมูลจากการตรวจสอบจากสถาบันการเงิน วัตถุประสงค์ก็คือฐานการประมวลผลเข้าข้อยกเว้นตามมาตรา ๒๔ (๔) แล้วมีการส่งต่อให้กับฝ่ายงานที่ทำหน้าที่ในการวิจัยเพื่อประโยชน์ในการออก	การแจ้งนั้นอาจจะแจ้งไปตั้งแต่ตอนที่ได้ข้อมูลมา คือควรจะทำให้เสร็จตั้งแต่ครั้งแรก	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	นโยบาย ธนาคารแห่งประเทศไทยเป็นผู้ควบคุมข้อมูล แต่การเก็บข้อมูลเข้ามาครั้งแรกได้มาด้วยฐานของมาตรา ๒๔ (๔) ส่งต่อให้อีกฝ่ายงานหนึ่งเพื่อประโยชน์ในการวิจัยออกนโยบายเข้ากรณีมาตรา ๒๔ (๑) เช่นนี้ จะต้องไปแจ้งเจ้าของข้อมูลอีกหรือไม่		
๓๓	เรื่องข้อมูลพนักงานบริษัทซึ่งหลายๆ บริษัทก็ยังมีการเข้าออกงานโดยการ Scan ลายนิ้วมือ ต้องขอ Consent จากพนักงานหรือไม่	พนักงานต้อง Scan ลายนิ้วมือเข้าออก คือ กำหนดว่ามาตรการเข้าออกงานนั้นจะใช้วิธีการนี้ก็อธิบายความจำเป็น แต่การจะเก็บก็ต้องมีขั้นตอนการขอ Consent ที่ชัดเจนตั้งแต่ตอนแรกเพื่อบอกว่าจะมีการใช้งานแบบนี้เกิดขึ้น	
๓๔	ข้อมูลบัตรประชาชน ในบัตรประชาชนจะมีข้อมูล เช่น ศาสนาซึ่งเป็นข้อมูล Sensitive การเก็บข้อมูลไม่ว่าจะเป็นภาพถ่าย สามารถดำเนินการอย่างไร	เป็นคำถามในทางปฏิบัติ โดยหลักคือเก็บเท่าที่จำเป็น ถ้าไม่อยากได้ก็หาทางที่จะไม่เก็บมัน จะไม่เก็บด้วยวิธีการไหน หรือถ้ามีประเด็นเกี่ยวกับธนาคารแห่งประเทศไทยก็ควรจะพูดคุยกัน	
๓๕	กรณีข้อมูลธรรมดากับ Sensitive มีปัญหาข้อมูลรั่วไหล จะมีผลอย่างไรบ้าง	ถ้ากรณีนั้นมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล แต่แน่นอนว่าถ้าเป็น Sensitive Data มันมีความเสี่ยงสูง เวลามีคดีเกิดขึ้นคนที่มีหน้าที่จะต้องแจ้งไปที่ซีอีโอ ควรจะมี contact แจ้งโดยตรงได้ หรือถ้าไม่มีก็คงต้องมีการประสานงานร่วมมือกัน	
๓๖	ในช่วงระหว่างนี้จนถึงปีหน้าทางกระทรวงหรือสำนักงานฯ จะมี guideline ออกมาบ้างหรือไม่	ถ้าตามแผนงานจะมี guideline ไว้แล้ว ไม่ว่าจะเป็นแผนเรื่องการจัดอบรมที่จะเกิดขึ้นแน่นอน การทำประชาสัมพันธ์ให้ความเข้าใจ กฎหมายลำดับรองก็เป็นอีกเรื่องหนึ่งที่จะต้องเร่งให้เกิดขึ้น	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
๓๗	ธนาคารจะส่งข้อมูลส่วนบุคคลมาที่บริษัท บริษัทเองก็จะมีการ process ในนามของธนาคาร ข้อมูลตรงนี้ทางบริษัทจะต้องทำ Consent หรือไม่ เพราะเราไม่ได้ deal กับลูกค้าโดยตรง	ท่านจะมีความผูกพันตามฐานการประมวลผล คือ ท่านทำแทน Controller ท่านทำอยู่ใน scope ที่เขาสั่ง เพราะฉะนั้นถ้าเค้าสั่งให้ท่านเก็บท่านก็ต้องเก็บตามที่เขาสั่ง แต่ทันทีที่ท่านทำเกินที่เขาสั่ง เช่น จะเก็บเกินอย่างนี้จะเกิดเป็นประเด็นว่าท่านจะต้องทำอย่างไร ซึ่งไม่แนะนำให้มีเหตุการณ์นี้เกิดขึ้น	
๓๘	ในกลุ่มผู้บังคับใช้กฎหมายคือในกลุ่มสถาบันการเงิน ในเรื่องที่จะต้องถ่ายทอดวิธีการไปยังลูกค้าซึ่งค่อนข้างที่จะเยอะมาก ในมุมการสื่อสารกับประชาชนที่เป็นลูกค้ากับธนาคาร ทางภาครัฐได้เตรียมที่จะช่วยไว้อย่างไรบ้าง	เป็นสิ่งที่ต้องช่วยกันทำ คงไม่สามารถที่จะบอกว่าเป็นหน้าที่ของคนใดคนหนึ่ง ระบบการสื่อสารของธนาคารกับลูกค้าเชื่อว่าการสื่อสารในรายละเอียดธนาคารจะทำได้ ส่วนรัฐบาลก็จะพยายามทำ การประชาสัมพันธ์ไม่ได้ประชาสัมพันธ์ในส่วนของผู้ประกอบการหรือไม่ใช่ประชาสัมพันธ์เฉพาะผู้ที่เป็นประชาชนทั้งสองฝ่ายจะต้องรู้และมีโอกาสได้ใช้พระราชบัญญัติฯ นี้เท่าๆ กัน	
๓๙	แนวทาง DPO ทางสำนักงานฯ อยากจะเห็นภาพของ DPO เป็นอย่างไรบ้าง	คำถามนี้เป็นคำถามที่ดีมากและใหญ่มาก เพราะว่า DPO ตอนนี้กำลังจะเป็นอาชีพใหม่ อาชีพยุค ๔.๐ ถ้าเป็นในแง่ของความเชี่ยวชาญแน่นอนว่าต้องเชี่ยวชาญจะต้องเป็นบุคคลและต้องเป็นบุคคลไทยหรือไม่ แนวโน้มถ้าอยากจะส่งเสริมอาจจะไม่ต้องบังคับ คือในแง่ต้องมีคนไทยอยู่ในองค์กรนี้อาจจะใช่แต่อาจจะเปิดให้เป็นบริษัทได้เพื่อให้กระบวนการนี้เป็นไปในเชิงธุรกิจมากๆ	
๔๐	ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ จะมีการกล่าวถึงมาตรฐานหรือมาตรการที่จะต้องทำเพื่อปกป้องข้อมูลส่วนบุคคล จะมีความเป็นไปได้หรือไม่ที่สำนักงานฯ จะช่วย	สำนักงานฯ จะต้องทำเรื่องนี้แน่นอน ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ไม่ได้ไปทำหน้าที่เปิดหรือปิดข้อมูล การเปิดหรือปิดเป็นเรื่องพระราชบัญญัติข้อมูลข่าวสารของราชการฯ เพียงแต่การจะเปิดหรือปิด	

ลำดับ	คำถาม	**คำชี้แจง** (ดร.ปิยะบุตร บุญอร่ามเรือง)	ข้อเสนอแนะ
	share มาตรการหรือมาตรฐานเหล่านี้เพื่อให้ผู้ประกอบการทำงานได้ง่ายขึ้น	ต้องมีมาตรฐานคุ้มครองข้อมูลซึ่งจะเป็นอีกประเด็นหนึ่ง	
๔๑	ถ้าเป็นการใช้โดยไม่ขอ Consent จะต้องมีการบันทึกข้อมูลตามมาตรา ๓๙ ใช่หรือไม่ และถ้ายังไม่มั่นใจว่าจะมีการบันทึกได้อย่างครบถ้วน ควรจะขอ Consent ไว้ก่อนเป็นหลักแล้วก็ใช้ข้อยกเว้นฐานข้อมูลการใช้เป็นตัวเสริมอย่างนี้จะดีกว่าหรือไม่	มาตรา ๓๙ ไม่ได้กำหนดว่าต้องบันทึกกรณีขอ Consent มาตรา ๓๙ กำหนดให้บันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยบันทึกข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ดังนั้น การเก็บรวบรวมนั้นไม่ต้องเป็น Consent ก็ได้ ถ้าท่านเห็นว่าตัวเองมีความสามารถไม่ครบถ้วนแสดงว่าท่านน่าจะต้องไปดูเรื่องว่าท่านน่าจะเป็นกิจการขนาดเล็ก ซึ่งจะยกเว้นเรื่องการบันทึกข้อมูลให้ได้ และอาจจะต้องรอคณะกรรมการฯ พิจารณาว่าหลักเกณฑ์และวิธีการจะเป็นอย่างไร	
๔๒	บริษัทที่เป็น SME ก็น่าจะมีผลกระทบเยอะ เนื่องจากว่ามาตรฐานที่ใช้ควบคุมข้อมูลออกมาบังคับแบบเข้มงวด SME ไม่มีทางทำได้ จะมีมาตรการอะไรหรือไม่ที่จะช่วยทำให้ผู้ประกอบการรายย่อยยังสามารถที่จะรับงานจากธนาคารได้ต่อไป	ทางสำนักงานฯ จะไปช่วยให้สามารถเดินต่อไปได้ เป็นงานที่อยู่ในแผนที่จะต้องช่วยให้ผู้ประกอบการรายเล็กสามารถที่จะทำตรงนี้ได้	
๔๓	ในกฎหมายระบุหน้าที่ของ DPO ไว้ ๔ ข้อ ทางสำนักงานฯ จะออก guideline ในตัว Detail ว่าหน้าที่ของ DPO ควรจะต้องรับผิดชอบหรือต้องพิจารณาหรือดูเรื่องอะไรบ้างหรือไม่	ต้องมี มันเป็นส่วนหนึ่งที่จะต้องมี ก็ต้องทำ ประเด็นนี้ทางสำนักงานฯ จะรับไว้	สำนักงานฯ จะรับประเด็นไว้