บันทึกการสัมมนา

ร่วมสร้างความพร้อมให้กับผู้ประกอบธุรกิจในตลาดทุน

เพื่อรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

<u>วิทยากร</u>

1. นาย กำพล ศรธนะรัตน์ ผู้ช่วยเลขาธิการ
2. ผู้ช่วยศาสตราจารย์ ดร. ปิยะบุตร บุญอร่ามเรือง ที่ปรึกษาและผู้เชี่ยวชาญด้าน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
3. นาย ปริย เตชะมวลไววิทย์ ผู้อำนวยการฝ่ายกำกับการขายผลิตภัณฑ์การลงทุน

<u>ผู้ดำเนินรายการ</u>

ดร. ไกรพิชิต เรืองศรีไชยะผู้อำนวยการฝ่ายจัดการและวิเคราะห์ข้อมูลตลาดทุน

<u>ดร. ไกรพิชิต</u>

การสัมมนาในวันนี้แบ่งออกเป็น 2 หัวข้อหลัก ได้แก่

1. ภาพใหญ่ของสำนักงานในการสนับสนุนและช่วยเหลือตลาดทุนเพื่อรองรับ PDPA
2. ประเด็นคำถามในเชิงปฏิบัติที่เกี่ยวกับภาคธุรกิจในตลาดทุน ซึ่งคำถามจะมาจาก Facebook live ครั้งก่อนหน้าและจากแบบประเมินความพร้อมของผู้ประกอบธุรกิจภายใต้การกำกับดูแลของก.ล.ต.

ซึ่งทางก.ล.ต. หวังเป็นอย่างยิ่งว่า คำตอบที่ได้จากการสัมมนาในวันนี้จะเพิ่มความรู้ความเข้าใจและสามารถนำไปปฏิบัติใช้ได้จริง นอกจากนี้หากผู้ประกอบธุรกิจอื่นนอกตลาดทุนมีข้อซักถามหรือข้อสงสัยในประเด็นลักษณะใกล้เคียงกัน ท่านสามารถนำแนวคำตอบหรือความเข้าใจนี้ไปประยุกต์ใช้ในธุรกิจของท่านได้ด้วยเช่นกัน

ก่อนหน้านี้สำนักงานก.ล.ต. ได้ทำการสำรวจความพร้อมในการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ของหน่วยงานภายใต้การกำกับดูแลทั้งหมด 276 บริษัทจาก 14 ประเภทธุรกิจ ดังนี้

1. บริษัทหลักทรัพย์
2. ผู้ให้บริการระบบคราวด์ฟันดิง (Funding Portal)

3. ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ICO Portal)
4. บริษัทหลักทรัพย์จัดการกองทุน
5. บริษัทสอบบัญชี
6. บริษัทหลักทรัพย์นายหน้าซื้อขายหน่วยลงทุน
7. บริษัทจัดอันดับความน่าเชื่อถือ
8. สมาคมตราสารหนี้ไทย
9. บริษัทหลักทรัพย์นายหน้าระหว่างผู้ค้าหลักทรัพย์
10. บริษัทที่ปรึกษาทางการเงิน
11. บริษัทประเมินมูลค่าทรัพย์สิน
12. ผู้จัดการกองทรัสต์
13. กลุ่มตลาดหลักทรัพย์แห่งประเทศไทย (SET GROUP)
14. ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล (Broker/ Exchange/ Dealer)

หัวข้อที่ใช้ในการประเมินถูกแบ่งเป็นหัวข้อหลักๆ 10 ด้าน ดังนี้

1. คำสั่งให้ดำเนินการเตรียมความพร้อมตาม พ.ร.บ. จากผู้บริหารระดับสูง
2. การแจ้งรายละเอียดการคุ้มครองข้อมูลส่วนบุคคล
3. การจัดทำ Consent Form
4. การประเมินกิจกรรมในการประมวลผล
5. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
6. การว่าจ้างให้บุคคลอื่นทำหน้าที่ประมวลผลข้อมูลแทน
7. การบันทึกรายการกิจกรรมประมวลข้อมูลส่วนบุคคล
8. การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
9. การบันทึกกิจกรรมการส่งข้อมูลไปยังต่างประเทศ
10. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ซึ่งการตอบคำถามจะเป็นการตอบเพียงว่าในแต่ละหัวข้อนั้น หน่วยงานของท่านมีหรือไม่ และพร้อมหรือไม่พร้อม เพื่อให้หน่วยงานหรือบริษัทเข้าใจในธุรกิจของตนเองมากขึ้นว่ามีความพร้อมด้านการจัดการข้อมูลส่วนบุคคลมากน้อยเพียงใด จากผลสำรวจพบว่าก.ล.ต. ได้รับแบบสอบถามกลับมา 70% ของบริษัททั้งหมด ซึ่งในจำนวนบริษัทที่ตอบกลับมานั้นมีความพร้อมอยู่ที่ 70% ส่วนธุรกิจที่มีความพร้อมสูง ได้แก่ กลุ่มบริษัทในเครือตลาดหลักทรัพย์แห่งประเทศไทย (SET Group) กลุ่มบริษัทหลักทรัพย์จัดการกองทุน กลุ่มบริษัทจัดอันดับความ

น่าเชื่อถือ กลุ่มผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ICO Portal) และกลุ่มผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ซึ่งผลประเมินความพร้อมแสดงให้เห็นว่าผู้ประกอบธุรกิจจำนวนมากมีความตื่นตัวกับพ.ร.บ. PDPA ในขณะเดียวกันยังคงมีบางบริษัทที่ไม่พร้อมและต้องเร่งดำเนินการมากขึ้น

เมื่อวานนี้ (21 พ.ค. 2563) ได้มีพระราชกฤษฎีกาเรื่องการบังคับใช้พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลประกาศออกมา ประกาศฉบับดังกล่าวมีผลให้ธุรกิจภายใต้การกำกับดูแลของก.ล.ต.ทั้ง 14 กลุ่มธุรกิจได้รับการเลื่อนการบังคับใช้หรือไม่

ผศ.ดร. ปิยะบุตร

สำหรับกลุ่มธุรกิจภายใต้การกำกับดูแลอยู่ในหัวข้อวงเล็บ 14 กิจการด้านการเงิน การธนาคารและการประกันภัยนั้น หากอธิบายในฐานะที่เป็นที่ปรึกษาของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ขอเรียนให้ทราบว่า พระราชกฤษฎีกานี้โดยเฉพาะรายการในบัญชีท้าย อ้างอิงจากรหัสมาตรฐานทางอุตสาหกรรมและบริการของประเทศไทย ซึ่งวงเล็บ 14 นั้นอยู่ในหมวด K คือกลุ่มที่เกี่ยวกับกิจกรรมทางการเงินและการประกันภัย ในแต่ละหมวดจะมีเลข 6 หลัก และถ้าเข้าไปดูในเลข 6 หลักจะพบว่า หมวดนี้ได้รวมกิจกรรมทั้งหมดของกลุ่มที่กล่าวข้างต้นแล้ว หากมีข้อสงสัยเพิ่มเติมท่านสามารถเข้าไปตรวจสอบจากรหัส 6 หลักนั้นได้ เจตนาคือต้องการให้ครอบคลุมกลุ่มงานที่เกี่ยวกับการเงิน การธนาคารและการประกันภัย ซึ่งรวมถึงงานที่เกี่ยวกับหลักทรัพย์ด้วย

ดร. ไกรพิชิต

เป็นที่ชัดเจนว่าธุรกิจที่อยู่ภายใต้การกำกับดูแลของสำนักงานก.ล.ต. ได้รับการเลื่อนการบังคับใช้ของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลไปอีก 1 ปี ซึ่งหมวดที่มีการเลื่อนบังคับใช้ได้แก่ หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล หมวด 5 การร้องเรียน หมวด 6 ความรับผิดทางแพ่ง และหมวด 7 บทกำหนดโทษ พระราษกฤษฎีกานี้ถูกกำหนดขึ้นเพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวง DES) กำหนด เมื่อพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลเลื่อนการบังคับใช้ออกไป ขอถามสำนักงานก.ล.ต.ในฐานะที่มีบทบาทเป็น regulator ว่ามีข้อแนะนำให้กับภาคธุรกิจในการเตรียมตัวก่อนที่กฎหมายจะประกาศบังคับใช้อย่างไร

นายกำพล

แม้ว่ากฎหมายจะมีการเลื่อนบังคับใช้ แต่บริษัทภายใต้กำกับก็ยังคงต้องพัฒนาอย่างต่อเนื่อง แนวคำถามในแบบประเมินความพร้อมที่สำนักงานก.ล.ต. ส่งให้กับบริษัททั้ง 14 กลุ่มนั้น อ้างอิงจาก 5 มาตราเป็นหลัก เพราะฉะนั้นแปลว่ามีหลายสิ่งที่ต้องเตรียมการและดำเนินการ และในแต่ละส่วนย่อมใช้เวลาในการเตรียมการเช่นกัน ผลการประเมินบริษัท 14 กลุ่ม แสดงให้เห็นว่าหลายกลุ่มบริษัทมีความพร้อมมาก สำหรับกลุ่มบริษัทที่มีความพร้อมน้อยกว่า ไม่ได้หมายความว่าไม่พร้อม บริษัทเหล่านั้นยังมีการเตรียมการและดำเนินการอยู่ กฎหมายทั้ง 5 มาตราสามารถขยายความได้ดังนี้

- มาตรา 23 จะต้องแจ้งเจ้าของข้อมูลส่วนบุคคลก่อนการเก็บรวบรวมข้อมูล (Privacy Policy) เป็นเรื่องของการจัดทำ privacy policy ขององค์กรเพื่อให้เจ้าของข้อมูลที่มาทำธุรกรรมทราบถึง ข้อมูลที่ต้องให้ วัตถุประสงค์ การใช้งานข้อมูล การเก็บข้อมูล ระยะเวลาจัดเก็บ การส่งต่อข้อมูลให้ผู้อื่น หรือแม้กระทั่งการติดต่อในกรณีที่เกิดปัญหา รวมถึงการแจ้งสิทธิของเจ้าของข้อมูลตามฐานกฎหมาย และสิทธิ์ในการเข้าถึงข้อมูล การทำลายข้อมูล
- มาตรา 24 กล่าวถึงหลักการเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลในแต่ละฐานการประมวลข้อมูลส่วนบุคคล เป็นเรื่องฐานประมวลผล ซึ่งโดยมากหน่วยงานที่อยู่ใต้กำกับดูแลจะเป็นฐานที่ต้องปฏิบัติตามกฎหมาย เช่น พ.ร.บ. หลักทรัพย์และตลาดหลักทรัพย์ หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง
- มาตรา 19 กรณีที่ต้องขอความยินยอมต้องมี consent form เป็นเรื่องความยินยอม อาจจะต้องมี consent form ในกรณีที่จะต้องขอข้อมูล
- มาตรา 37 มาตรการเพื่อความปลอดภัยของข้อมูล คืออย่าปล่อยให้ข้อมูลไม่มี Access Control เป็นเรื่องหน้าที่ของบริษัทที่มาขอข้อมูลจากสำนักงานก.ล.ต. จะต้องดูแลข้อมูล กล่าวคือมีความปลอดภัยหรือมี security policy การตรวจสอบข้อมูลเป็นระยะ ๆ หากมีข้อมูลที่จะต้องถูกลบ ข้อมูลเหล่านั้นได้ถูกลบหรือไม่ รวมไปถึงกรณีที่ข้อมูลถูกละเมิดทำให้รั่วไหลออกไป มีการแจ้งเจ้าของข้อมูลโดยไม่ชักช้าหรือไม่ ซึ่งอาจจะถูกกำหนดด้วยกฎหมายลูกที่คณะกรรมการ PDPA จะประกาศต่อไป แต่อย่างไรก็ตามแม้จะยังไม่มีกฎหมายลูก การเตรียมการนั้นสามารถดำเนินการไว้ก่อนได้
- มาตรา 39 ต้องมีการบันทึกกิจกรรมการประมวลข้อมูลส่วนบุคคลที่เรียกว่า Record of Processing Activities (ROP) เป็นเรื่องการบันทึกกิจกรรรม เมื่อมีการประมวลผลข้อมูลต้องมีการเก็บบันทึกกิจกรรมต่าง ๆ เพื่อให้มั่นใจว่า บริษัทหรือองค์กรที่ให้บริการทำอะไรกับข้อมูลส่วนบุคคลมากน้อยเพียงใด

ในการทำแบบสำรวจความพร้อมนั้นทางสำนักงานก.ล.ต. ได้อ้างอิงจาก 5 มาตราที่กล่าวมาข้างต้น ซึ่งคำถามที่ประเมินความพร้อมล้วนเป็นกิจกรรมที่บริษัทสามารถดำเนินการได้ตั้งแต่วันนี้ แม้ว่าจะมีการเลื่อนบังคับใช้ไปแล้วก็ตาม

ดร. ไกรพิชิต

ขอสรุปว่าแม้จะมีการเลื่อนการบังคับใช้ แต่อย่างไรก็ตามบริษัทต้องปฏิบัติตามที่พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนด การทำก่อนและพร้อมก่อนจะช่วยลดความเสี่ยงต่อการฝ่าฝืนหรือปฏิบัติไม่ครบตามข้อกฎหมาย นอกจากนี้ยังเป็นการให้ผู้บริหารและพนักงานบริษัทมีการปรับตัวและเตรียมความพร้อมได้ตั้งแต่ก่อนที่กฎหมายจะบังคับใช้ในปีหน้า สิ่งสำคัญคือการปฏิบัติตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้อย่างครบถ้วนถูกต้องจะส่งผลให้บริษัทของท่านมีความน่าเชื่อถือกับลูกค้ามากขึ้น

ขอถามอ.ปิยะบุตรในฐานะที่เป็นที่ปรึกษาให้กับกระทรวง DES ในเรื่องนี้โดยเฉพาะ อยากให้อ.ปิยะบุตรแนะนำหรือให้ความคิดเห็น ถึงสิ่งที่ภาคธุรกิจควรเน้นเป็นพิเศษ สิ่งที่น่าเป็นห่วง หรือหัวข้อที่อาจจะใช้เวลามากซึ่งผู้ประกอบธุรกิจอาจไม่ได้คำนึงถึง พร้อมทั้งยกตัวอย่างหรือจากประสบการณ์ที่สามารถบอกเล่าได้

ผศ.ดร. ปิยะบุตร

สิ่งที่นายกำพลอธิบายมาข้างต้นนั้นดีมากและชัดเจนว่าผู้ประกอบการจะต้องทำอะไรบ้าง แต่ก่อนที่จะเสนอข้อแนะนำ ขออธิบายถึงข้อดีของ PDPA ว่า ณ ตอนนี้มีพ.ร.บ. และพระราชกฤษฎีกา ซึ่งพ.ร.บ.มีผลบังคับ แต่พระราชกฤษฎีกานั้นเป็นประกาศลูกของพ.ร.บ.ซึ่งแจ้งในส่วนที่บังคับให้เลื่อนออกไป ถ้าอธิบายถึงกฎหมายเปรียบเสมือนการเขียน coding เขียนโปรแกรม ส่วนแรกมีการกำหนดหลักการหรือ definition ไว้ก่อนซึ่งก็คือ พ.ร.บ. และอีกส่วนคือ พระราชกฤษฎีกาซึ่งไม่ได้กำหนดหลักการใด ๆ แต่แจ้งว่าส่วนที่จะลงโทษนั้นให้เลื่อนออกไป นั่นหมายความว่านิยามความหมายที่ประกาศไว้ตั้งแต่ปีที่แล้วยังมีผลอยู่ ตัวอย่างเช่น consent ยังมีความหมายเหมือนเดิมตาม PDPA กล่าวคือ consent ตาม PDPA จะต้องชัดเจน อ่านง่าย เข้าใจง่าย จะต้องเป็นอิสระให้เลือกได้ จะต้องปฏิเสธและจะถอนเมื่อใดก็ได้ นิยามนี้ยังคงเดิมไม่มีการเปลี่ยนแปลง แต่ที่ประกาศว่า ถ้าไม่ได้ทำตามจะยังไม่ลงโทษก็คือมีการขยายออกไป นอกจากนี้ PDPA ยังมีฐานกฎหมายอื่นนอกเหนือจาก consent นั่นคือ contract และ legitimate interest ซึ่งนิยามไว้แล้ว และผู้ประกอบการจะได้รับประโยชน์จาก 2 ฐานกฎหมายนี้โดยไม่ต้องใช้ consent เนื่องจากมีฐานกฎหมายเฉพาะ กล่าวคือ ถ้าเป็นการทำตามสัญญา (contract) หรือเป็น legitimate interest นั้นไม่ต้องขอ consent แต่อย่างใด แต่หากไม่เข้าใจนิยามดังกล่าวและยังใช้ consent แบบเดิมที่ครอบคลุมทุกอย่างว่าต้องขอความยินยอม จะไม่สามารถทำได้เนื่องจากนิยามความหมายได้กำหนดแล้วตาม พรบ. ดังนั้นผู้ประกอบการควรนำข้อดีของ PDPA ข้อนี้มาใช้ให้เกิดประโยชน์ มีคำถามว่า ถ้ากลับไปใช้ consent form เดิมได้หรือไม่ คำตอบคือ เป็นสิ่งที่ไม่ควรทำอย่างยิ่งเพราะไม่เกิดประโยชน์กับภาคธุรกิจ เพราะ

จากที่เดิมใช้ consent form หากมันคือ contract ในปัจจุบัน ผู้ประกอบการควรเปลี่ยนเป็น contract หรือ legitimate interest จะได้ประโยชน์จากเรื่องนี้และมีความชัดเจนมากกว่า

สำหรับข้อแนะนำในเรื่องนี้คือ ตามหลักการแนะนำให้ทำ ROP (Record of Processing Activities) ให้เสร็จก่อนเพื่อจะได้ทราบแนวทางในการทำนโยบาย (policy) ต่อไป แต่ช่วงเวลา 1 ปีที่ผ่านมาการทำตามขั้นตอนซึ่งใช้เวลานานนั้นเป็นไปได้ยาก ดังนั้นต่างคนจึงต่างเร่งทำส่วนของตนเอง ไม่ว่าจะเป็นนโยบาย (policy) consent ฯลฯ เพราะฉะนั้นเมื่อปีนี้มีการขยายเวลา การทำตามขั้นตอนที่กล่าวข้างต้นจึงสามารถทำได้ อันดับแรกที่บริษัทควรเน้นคือ ROP เพราะ ROP จะบอก gap และผู้ประกอบการจะรู้ว่าข้อมูลใดไม่ควรเก็บหรือควรถูกดำเนินการลบออกไปหรือ process การทำงานควรจะถูกปรับปรุงอย่างไร ขณะเดียวกัน policy ก็จะไม่ต้องทำโดยไม่รู้ gap กล่าวคือสามารถที่จะรอ gap ก่อนแล้วจึงเขียนออกมาได้ แต่สิ่งที่อยากเน้นในระยะนี้โดยในปีที่แล้วมีการพูดถึงน้อยมากคือเรื่องสิทธิของเจ้าของข้อมูลซึ่งสำคัญมาก เพราะในระยะหลังคนเริ่มรู้เรื่องนี้และมีคำถามมากขึ้น คาดว่าจะมีหลายคนจะมาขอใช้สิทธิ และเนื่องจากเราไม่เคยจัดการเรื่องนี้กันมาก่อน หากไม่รีบดำเนินการในช่วงที่ยังมีเวลา รอจนถึงวันที่ 1 มิ.ย. 64 เปิดให้คนใช้สิทธิแล้วมีจำนวนคนมาใช้สิทธิเป็นร้อยคนบริษัทจะรับไม่ไหว ดังนั้นปีนี้ต้องเป็นช่วงเวลาของการทดลองให้คนใช้สิทธิ เมื่อถึงเวลาจะได้ไม่เกิดความตื่นตระหนกและไม่กระทบกับกระบวนการทำงานมากเกินไป

<u>ดร. ไกรพิชิต</u>

สรุปว่าเรื่องที่ต้องทำเป็นอันดับแรกคือ ROP (Record of Processing Activities) เพื่อทำการตรวจสอบ process หรือจัดการข้อมูลส่วนบุคคลที่อยู่ในการควบคุมของผู้ประกอบการซึ่งมีอยู่จำนวนมาก ข้อสังเกตหนึ่งคือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลนั้นเป็นกฎหมายใหม่สำหรับประเทศไทย ทำให้ความเข้าใจในหลักวิธีคิดที่จะนำไปสู่การปฏิบัติอาจมีความติดขัดหรือความไม่ชัดเจนสูง ตามที่อ. ปิยะบุตรได้กล่าวมาเช่น เรื่องฐานกฎหมายสำหรับการนำข้อมูลส่วนบุคคลไปใช้ประมวลผล มีทั้ง consent contract และ legitimate interest การเข้าใจและการประยุกต์ใช้ซึ่งจะนำไปสู่การปฏิบัติตามกฎหมาย PDPA ในประเทศไทยนั้น ขอถามอ. ปิยะบุตรว่า มีการเตรียมการในเรื่องนี้อย่างไรเพื่อช่วยผู้ประกอบธุรกิจในการเตรียมความพร้อมเพื่อนำไปสู่มาตรฐานใหม่ในการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

<u>ผศ.ดร. ปิยะบุตร</u>

ถ้าตอบในนามสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) สิ่งที่พอจะทราบคือตอนนี้ มีการแต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว ซึ่งเปรียบเสมือนข้อต่อที่นำไปสู่เรื่องอื่น ๆ ต่อไป กล่าวคือเมื่อมีการแต่งตั้งคณะกรรมการเรียบร้อย กระบวนการสรรหาเลขาธิการสำนักงานจะสามารถดำเนินการได้ต่อ รวมไปถึงการรับสมัครเจ้าหน้าที่และงบประมาณก็จะเกิดขึ้น ที่ผ่านมานั้นทางสำนักงานไม่ได้นิ่งนอนใจ สิ่งที่ปลัดกระทรวง DES ดำเนินการอยู่ เรื่องแรกจะเป็นการทำตามพระราชกฤษฎีกาเรื่องมาตรฐานความปลอดภัยที่กล่าวว่าไม่มีใครได้รับข้อยกเว้น และอีกเรื่องจะเกี่ยวกับการช่วยเหลือ แนวปฏิบัติในการดำเนินงาน และการออกกฎหมายลูกซึ่งจะเป็นกลุ่มงานแรกๆที่จะดำเนินการ เพราะฉะนั้นคาดว่าจะเห็นกฎหมายลูกและ guideline จากสคส. ในปีนี้

ดร. ไกรพิชิต

ดังนั้นช่วง 1 ปีที่จะมาถึงนี้จะเห็นความชัดเจนจากกฎหมายลูกออกมามากขึ้น สคส.เองซึ่งเป็น regulator โดยตรงของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลนั้นไม่ได้นิ่งนอนใจ ยังคงทำงานอย่างต่อเนื่องเพื่อให้เกิดความชัดเจน รวมไปถึงให้ความช่วยเหลือภาคเอกชนในการปฏิบัติตามพ.ร.บ.ฉบับนี้ ขอถามนายกำพลว่า สำนักงาน ก.ล.ต. มีแนวทางและการเตรียมความพร้อมในการให้ความช่วยเหลือหรือสนับสนุนภาคธุรกิจในตลาดทุนอย่างไร

นายกำพล

สำนักงานก.ล.ต.มีเกณฑ์ด้าน IT security ที่เกี่ยวข้องกับเรื่อง governance และ information security ที่อ้างอิงตามมาตรฐาน ISO27001 อยู่แล้ว ซึ่งลักษณะจะเป็นข้อมูลกลมๆ เช่น กรณีข้อมูลถูกโจรกรรมหรือระบบเครือข่ายถูกเจาะจนทำให้เกิดการเข้าถึงข้อมูลและข้อมูลรั่วไหล บริษัทที่อยู่ภายใต้กำกับมีหน้าที่ต้องรายงาน แก้ไขและเยียวยาภายใต้เกณฑ์ข้อกำหนดของสำนักงานก.ล.ต แต่เมื่อมีกฎหมาย PDPA เกิดขึ้น ฐานะของสำนักงานก.ล.ต.จะต้องเปลี่ยนจากที่เป็น regulator มาเป็นหนึ่งในผู้ที่ถูกกำกับด้วย PDPA เช่นกัน

ในช่วง 1 ปีที่ผ่านมา สำนักงานก.ล.ต. มีการเตรียมการอยู่หลายภาคส่วน เช่น การทำทะเบียนข้อมูล การจำแนกข้อมูลส่วนบุคคล การจัดทำ privacy policy และเนื่องด้วยสำนักงานก.ล.ต. เป็นหน่วยงานภาครัฐ จึงมีการจัดทำ privacy policy ภายใต้พระราชกฤษฎีกา มาตรา 35 ของพ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์อยู่แล้ว แต่เมื่อมีพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ก็จะมีสิ่งที่จะต้องทำเพิ่มเติม เช่น เรื่อง consent form เรื่อง privacy notice หรือ privacy policy จะต้องละเอียดมากขึ้นโดยเฉพาะอย่างยิ่งในเรื่องของการดูแลข้อมูลจะต้องครอบคลุมตลอด life cycle ซึ่ง ROP หรือ Record of Processing Activities ดังที่อ. ปิยะบุตรกล่าวไปข้างต้น จะสามารถช่วย

จัดการในเรื่องดังกล่าวได้ อย่างไรก็ตามการดูแลข้อมูลตลอด life cycle นั้นมีสิ่งที่ต้องดำเนินการอีกมากและล้วนเป็นสิ่งที่เกี่ยวเนื่องกับเทคโนโลยี ระบบอัตโนมัติ เข้าใจว่าเหตุผลหนึ่งที่ท้ายประกาศของพระราชกฤษฎีกาที่เลื่อนคือการกล่าวถึงเทคโนโลยีขั้นสูง โดยเทคโนโลยีขั้นสูงจะเป็นคำตอบของเรื่อง gap ของอ. ปิยะบุตรและสิ่งที่ต้องทำเพิ่ม กล่าวคือต้องมีการแก้ไขระบบ ทำให้ระบบรองรับการใช้สิทธิ์ของเจ้าของข้อมูล ซึ่งจะนำไปสู่คำถามที่ว่า ทำมากน้อยเพียงใดจึงจะเพียงพอ ตอนนี้สมาคมและหน่วยงานต่าง ๆ มีการจ้างที่ปรึกษาเข้ามาช่วยในเรื่องการกำหนดมาตรฐาน แต่เนื่องจากหน่วยงานภายใต้กำกับของสำนักงานก.ล.ต. มีถึง 14 กลุ่มธุรกิจ การทำให้เป็นมาตรฐานเดียวกันนั้นเป็นเรื่องยากเพราะบริษัทมีทั้งขนาดเล็กและขนาดใหญ่ ความจำเป็นในการใช้ข้อมูลส่วนบุคคลก็แตกต่างกัน ดังนั้นสำนักงานก.ล.ต. และภาคอุตสาหกรรมจำเป็นต้องหารือร่วมกัน นอกจากนี้ยังมี regulator อื่นได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) และ สคส. ซึ่งคณะทำงานทั้ง 4 หน่วยงานรวมถึงก.ล.ต. จะต้องร่วมมือกันจัดระเบียบ ตัวอย่างเช่น การจัดทำระบบให้เพียงพอและครบถ้วน เพื่อรองรับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ตามฐานความจำเป็น

อีกประเด็นที่สำคัญคือคำถามเรื่องการ comply กับสคส. ในเรื่องนี้สำนักงานก.ล.ต. มีหน้าที่ช่วย facilitate เพื่อให้บริษัททำงานได้อย่างราบรื่นไม่มีปัญหาอยู่แล้ว แต่หากภาคอุตสาหกรรมมีประเด็นปัญหาอะไรเป็นพิเศษ และคิดว่าการสัมมนาในวันนี้อาจจะยังไม่ตอบโจทย์ ทางสำนักงานก.ล.ต. ก็ยินดีรับข้อคิดเห็นเพื่อตอบคำถาม ให้คำแนะนำหรือให้ความร่วมมือกับทุกหน่วยงาน เพราะนอกจากอ. ปิยะบุตรจะเป็นที่ปรึกษาให้กับสคส. และสำนักงาน ก.ล.ต. แล้ว ยังเป็นตัวแทนของ สคส.ในการประชุมร่วมกันของ 3 regulator อีกด้วย ยิ่งไปกว่านั้นท่านเลขาธิการของก.ล.ต. นางสาวรื่นวดี สุวรรณมงคลก็เป็นหนึ่งในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทำให้ทาง ก.ล.ต. สามารถช่วยประสานงานเพื่อเป็นข้อต่อตรงกาลาง สังคมของเราเป็นสังคมของ compliance สูงสุด เมื่อใดก็ตามที่ปิด compliance จะเป็นเรื่องบทลงโทษซึ่งเป็นสิ่งที่เราตระหนักกันดี ในส่วนของสำนักงานก.ล.ต. จะมีดร. ไกรพิชิตจากฝ่ายข้อมูลที่จะช่วยเป็นหัวหน้ารับผิดชอบสำหรับงานนี้ด้วย

<u>ดร. ไกรพิชิต</u>

เป็นที่ชัดเจนว่าทางสำนักงานก.ล.ต. มีการ comply ตามกฎหมายและส่งเสริมให้ผู้ประกอบธุรกิจในตลาดทุนต้อง comply ตามด้วยเช่นเดียวกัน นอกจากนี้ทางก.ล.ต. ยังมีความร่วมมือกับ regulator อื่น ๆ ได้แก่ ธปท. คปภ. และ สคส. ในการพัฒนาระบบหรือการ comply ตามกฎหมายในภาคของการเงินให้เป็นไปอย่างชัดเจน คำถามสุดท้ายสำหรับภาพใหญ่คือ การทำงานของ regulator ในการกำกับดูแลหน่วยงานในหลายภาคส่วนรวมถึงก.ล.ต. เอง มีความจำเป็นจะต้องเรียกขอข้อมูลจากผู้ประกอบธุรกิจให้ส่งข้อมูลมายังตัว regulator ซึ่งไม่อาจ

หลีกเลี่ยงการส่งข้อมูลส่วนบุคคลของลูกค้าของธุรกิจนั้น ๆ ได้ ขอถามอ.ปิยะบุตรว่าการส่งข้อมูลส่วนบุคคลให้กับ regulator ผ่านทางผู้ประกอบธุรกิจเพื่อใช้ประกอบการปฏิบัติหน้าที่ ถือเป็นการขัดต่อพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่

ผศ.ดร. ปิยะบุตร

ก่อนอื่นขออธิบายพื้นฐานของพ.ร.บ. PDPA ว่าหลักการของ PDPA ไม่ได้เปลี่ยนแปลงวิธีการทำงานเดิมหรือการใช้ข้อมูลส่วนบุคคลตามที่กฎหมายอื่นกำหนดอยู่เดิมว่าต้องทำ เพราะกฎหมายอื่นโดยหลักการจะมีการกำหนดอยู่แล้วว่าจำเป็นต้องใช้ข้อมูล เช่น กรณีการทำ KYC/CDD (Know Your Customer/Customer Due Diligence) มีเงื่อนไขในการดำเนินการอยู่แล้วว่าจำเป็นจะต้องกำกับดูแลและตรวจสอบ โดยที่พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลไม่ได้เปลี่ยนวัตถุประสงค์หรือการดำเนินการทำ KYC/CDD แต่อย่างใด แต่เป็นไปตามมาตรา 24 (4) Public task คือเป็นการดำเนินการของหน่วยงานรัฐที่ทำตามภารกิจต้องส่งข้อมูลให้เพื่อการจัดการ เมื่อมีฐานกฎหมายนี้ประกาศออกไป ผู้ประกอบการจะต้องดำเนินการตามประกาศฉบับนี้ตามเกณฑ์ที่ regulator กำหนด ปัญหาคือที่ผ่านมาไม่มีการสื่อสารออกไปให้เห็นถึงความชัดเจนของการใช้อำนาจและการต้องใช้ข้อมูล เมื่อมีการกำหนดขึ้น ผู้ประกอบการจะเกิดความสับสนว่าจะต้องเอาข้อมูลไปใช้ด้วยเหตุผลใด มีความเกี่ยวข้องและความจำเป็นอย่างไร เนื่องจากในอดีตไม่มี privacy policy อธิบายมาก่อน ซึ่ง privacy policy ที่กำลังดำเนินการกันอยู่นี้จะเป็นสิ่งที่แจ้งให้ทราบว่าข้อมูลถูกใช้ตามกฎหมาย และมีการระบุว่าจะต้องเก็บข้อมูลใดบ้าง หลักการพื้นฐานของ PDPA คือต้องการให้เจ้าของข้อมูลรับทราบว่าข้อมูลนั้นจะถูกนำไปใช้ทำอะไร และหากเจ้าของข้อมูลไม่ทราบข้อมูลดังกล่าวก็ไม่ควรจะถูกนำมาใช้ยกเว้นแต่ว่าผู้ประกอบการจะสามารถอธิบายได้ สิ่งนี้คือสาระสำคัญของเรื่องทั้งหมด หากมีความเข้าใจในส่วนนี้แล้วสิ่งที่ต้องดำเนินการต่อจะค่อนข้างง่าย เพราะฉะนั้นวิธีการคือจะต้องแจ้งให้ลูกค้าทราบตั้งแต่แรก

ดร. ไกรพิชิต

โดยสรุปคือหากผู้ประกอบธุรกิจเคยส่งข้อมูลของลูกค้าให้กับ regulator อยู่แล้วก็ยังคงเหมือนเดิมไม่เปลี่ยนแปลง พ.ร.บ. PDPA เพียงมาช่วยต่อยอดให้เกิดความชัดเจนมากขึ้น และมาช่วยเสริมว่าเจ้าของข้อมูลส่วนบุคคลนั้นจะต้องรับทราบว่ามีการส่งข้อมูล

สำหรับคำถามในภาพใหญ่ของสำนักงานนั้น คิดว่าน่าจะครอบคลุมพอสมควรแล้ว ดังนั้นขอนำเข้าสู่หัวข้อหลักที่ 2 คือประเด็นคำถามในเชิงปฏิบัติเกี่ยวกับภาคธุรกิจในตลาดทุน เริ่มจากกลุ่มธุรกิจแรกคือกลุ่มธุรกิจที่เกี่ยวกับการขายผลิตภัณฑ์การลงทุน ขอถามนายปริย ให้ช่วยอธิบายลักษณะของธุรกิจการขายผลิตภัณฑ์การลงทุน การประกอบธุรกิจรวมถึงผู้ที่ได้รับอนุญาตจากสำนักงาน ซึ่งกิจกรรมเหล่านี้ทั้งทางธุรกิจเองและผู้ประกอบธุรกิจซึ่งได้รับอนุญาตจากสำนักงานก.ล.ต. ล้วนเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งสิ้น

นายปริย

LBDU เป็นธุรกิจที่เกี่ยวกับนายหน้าซื้อขายหน่วยลงทุนซึ่งปัจจุบันประชาชนสามารถไปซื้อหน่วยลงทุนได้ที่ธนาคารหรือกับบริษัทที่ให้บริการขายหน่วยลงทุน กล่าวคือมีช่องทางการขายที่ใหญ่มาก และนี่เป็น 1 ใน 14 ภาคธุรกิจที่วิทยากรได้กล่าวข้างต้นว่ามีการสอบถามเรื่องความพร้อมในการปฏิบัติตามกฎหมาย PDPA สาเหตุที่ต้องอธิบายและยกตัวอย่างธุรกิจนี้ให้เห็นก่อนว่ามีเรื่องราวอย่างไรและเกี่ยวข้องกับ PDPA อย่างไรบ้างเนื่องจากธุรกิจนี้เกี่ยวข้องกับผู้ลงทุนค่อนข้างมาก เป็นที่ทราบกันดีว่าผู้ประกอบการในตลาดทุนคือบริษัทหลักทรัพย์ บริษัทจัดการลงทุน และธนาคารพาณิชย์ แต่ในความเป็นจริงตัวแทนขายหน่วยลงทุน ตัวผู้ติดต่อผู้ลงทุนหรือผู้แนะนำการลงทุนนั้นถือเป็นบุคคลากรจำนวนหลักหมื่นคนที่จะต้องขึ้นทะเบียนกับก.ล.ต. กรณีที่บริษัทเหล่านี้ให้บริการเปิดบัญชีซื้อขายกับลูกค้า ลูกค้าไปซื้อกองทุนต้องเปิดบัญชีหรือการซื้อขายหลักทรัพย์ต้องติดต่อบริษัทหลักทรัพย์ล้วนต้องเจอกับ IC ทั้งสิ้น เรียกได้ว่าเป็นจุดที่เก็บรวบรวมข้อมูลจากด้านผู้ลงทุนเข้ามาที่บริษัทหลักทรัพย์ ในการเปิดบัญชีบริษัทจะมีแบบฟอร์มให้ในการเก็บข้อมูลผู้ลงทุนว่าจะต้องมีข้อมูลอะไรบ้างที่บริษัทหลักทรัพย์ต้องการ การประเมินความพร้อมของผู้ลงทุน ข้อมูลเหล่านี้จัดเป็นข้อมูลส่วนบุคคลที่บริษัทหลักทรัพย์มีให้บริการนานแล้วเพียงแต่ปัจจุบันจะต้อง comply ตามพ.ร.บ. PDPA ในตอนต้นอ. ปิยะบุตรได้อธิบายว่าข้อมูลพวกนี้เป็นข้อมูลสำคัญที่บริษัทต้องใช้ในการประเมินความพร้อมของลูกค้า ที่ผ่านมาอาจเรียกว่าเป็นการขอความยินยอม แต่ตอนนี้จะต้องขยับมาในส่วนที่เป็น contract ส่วนเรื่อง IC จะเป็นผู้ติดต่อผู้ลงทุน บุคคลกลุ่มนี้จะต้องมีความรู้เกี่ยวกับกฎหมาย PDPA ค่อนข้างมาก นอกจากนี้ปัจจุบันมีการบริการผ่านทางออนไลน์ ทำให้หลายบริษัทเปลี่ยนรูปแบบเป็นการให้บริการผ่านแอพพลิเคชั่นผ่านอินเตอร์เน็ต ซึ่งนี่จะเป็นอีกจุดหนึ่งที่จะต้องเกี่ยวข้องกับกฎหมาย PDPA ด้วยเช่นกัน

ในปัจจุบันมีหลายบริษัทที่เริ่มดำเนินการตามพ.ร.บ. PDPA ไปบ้างแล้ว เท่าที่ได้ดู privacy policy ของหลายบริษัทบนเว็บไซต์แสดงให้เห็นว่า บริษัทที่มองว่ากฎหมาย PDPA เลื่อนแล้วไม่จำเป็นต้องรีบดำเนินการอาจจะส่งผลเสียทำให้ลูกค้ามองว่าบริษัทไม่พร้อมในเรื่องนี้และตัดสินใจไปหาบริษัทอื่นที่มีความพร้อมมากกว่าเพื่อให้บริษัทที่พร้อมดำเนินการดูแลเรื่องสิทธิ์และข้อมูลของผู้ลงทุน เพราะฉะนั้นบริษัทที่ยังไม่เริ่มดำเนินการหรือ

รอไปช่วงใกล้ๆอาจจะต้องเปลี่ยนแนวความคิด เพราะหลายบริษัทมี awareness แล้วว่าจะต้อง comply ตามกฎหมาย ตอนนี้กฎหมายหลักประกาศออกมาเรียบร้อยแล้วและกฎหมายลูกกำลังทยอยออกมา ซึ่งสำนักงานก.ล.ต เองพยายามเป็นศูนย์กลางเพื่ออำนวยความสะดวกให้กับกลุ่มผู้ประกอบการ รวมถึงสนับสนุนการจัดกิจกรรมเกี่ยวกับการให้ความรู้มาอย่างต่อเนื่อง เพื่อความเข้าใจเบื้องต้นว่ากลุ่มบริษัทมีความสงสัยอย่างไรบ้างในเรื่องการปฏิบัติตามกฎหมาย PDPA หลังจากนี้สำนักงานก.ล.ต. จะต้องค้นหาคำตอบสำหรับคำถามที่ผู้ประกอบการได้สอบถามเข้ามาจากภาคอุตสาหกรรมทั้ง 14 กลุ่ม พร้อมทั้งสรุปรวบรวมและโพสบนเว็บไซต์ของสำนักงานก.ล.ต. เพื่อให้บริษัทเห็นถึงแนวทางในการดำเนินการต่อไป

คำถามที่สรุปมาหลักๆเกี่ยวกับกฎหมายที่เพิ่งจะเข้ามามีผลเริ่มบังคับใช้ ซึ่งการดูแลข้อมูลของผู้ลงทุนเป็นพื้นฐานที่ทำกันมานานแล้ว หากดูแลไม่ดีอาจถูกฟ้องเรื่องการละเมิดได้ เมื่อกฎหมาย PDPA ถูกกำหนดขึ้นบริษัทจะต้องพิจารณาการ comply ให้ถูกต้องตามกฎหมายและการดูแลลูกค้าเก่าที่มีมาก่อนหน้าที่จะประกาศใช้กฎหมาย PDPA เพราะผู้ลงทุนในตลาดทุนนั้นมีจำนวนเป็นหลักล้านคน ดังนั้นบริษัทจะต้องหาวิธีดำเนินการในกรณีลูกค้าเก่าและลูกค้าใหม่ที่จะรับเข้ามาเพื่อให้เป็นไปตามกฎหมาย PDPA ขอถามอ. ปิยะบุตรว่า บริษัทต้องดูแลลูกค้าเก่าอย่างไร หรือต้องเข้าไปติดต่ออย่างไร เนื่องจากที่ผ่านมาจำนวนลูกค้ามีค่อนข้างมากและหลายคนเป็นลูกค้าที่ไม่ได้มีการติดต่อมานาน

<u>ผศ.ดร. ปิยะบุตร</u>

พ.ร.บ. PDPA ค่อนข้างยืดหยุ่นกว่า GDPR เพราะ GDPR จะระบุว่าทุกสิ่งเริ่มต้นจากศูนย์คือเริ่มต้นใหม่หมด แต่สำหรับ PDPA ตามมาตรา 95 ระบุว่าถ้าสิ่งใดที่มีอยู่เดิมเป็น consent ผู้ควบคุมข้อมูลสามารถใช้ต่อไปได้ แต่จะต้องเปิดโอกาสให้เจ้าของข้อมูลมาถอนความยินยอมได้ เพราะฉะนั้นลูกค้าเก่าในความหมายนี้คือได้ consent อยู่เดิมจะไม่มีปัญหา แต่เนื่องจากมีพระราชกฤษฎีกาความซับซ้อนก็จะมีมากขึ้น กล่าวคือถ้ากรณีไม่มีพระราชกฤษฎีกา ณ วันที่ 27 พ.ค. นี้ consent เดิมก็คือ contract และจากที่บริษัทเคยระบุว่า ทางบริษัทขอความยินยอมเพื่อให้บริษัทนำข้อมูลของลูกค้าไปใช้เพื่อพัฒนาบริการและอื่นๆที่บริษัทเห็นสมควร คำว่า “อื่นๆที่บริษัทเห็นสมควร” จะไม่เข้านิยามของมาตรา 19 เพราะฉะนั้นจะใช้ไม่ได้อีกต่อไป แต่ส่วนที่ระบุว่า “เพื่อพัฒนาบริการ” นั้นยังใช้ได้อยู่ ซึ่งถ้าเป็น GDPR จะประกาศว่าไม่สามารถใช้ได้ แต่เนื่องจากเป็นกฎหมายไทยซึ่งระบุไว้ชัดว่าสามารถใช้ต่อไปได้แต่ต้องเปิดโอกาสให้เจ้าของข้อมูลมีสิทธิถอนความยินยอม ดังนั้นลูกค้าเก่าที่ได้เคย consent นั้นก็จะยังใช้ได้ต่อไป สำหรับวันนี้มีพระราชกฤษฎีกา ซึ่งเลื่อนออกไปอีก 1 ปี ระยะเวลาระหว่างนี้ถ้า consent เกิดก่อน 27 พ.ค. ความหมายจะยังเหมือนกับที่ได้อธิบายก่อนหน้า แต่หาก consent เกิดระหว่างปี 63 – 64 จะมีประเด็นว่าไม่สามารถเขียนอย่างเดิมได้อีกต่อไป เพราะว่านิยามของ consent นั้นมีผลบังคับใช้แล้ว ถ้ายังระบุ

แบบเดิมจะแสดงให้เห็นถึงการไม่ปฏิบัติตามคือมีความหมายเป็นอย่างอื่น เพราะฉะนั้นในความหมายนี้ของลูกค้าเก่า กฎหมายไทยประกาศว่าให้ใช้ต่อไปได้ในกรณีของ consent ข้อสังเกตคือหลักการนี้หมายความเฉพาะ consent แต่ในพ.ร.บ. PDPA มีอะไรมากกว่า consent นั่นคือลูกค้าเก่าที่ได้ให้ consent ไว้ความจริงแล้วเป็น contract หรือไม่ เก่าในที่นี้หมายถึงยัง active อยู่หรือไม่ ถ้ายัง active จะยังเป็น contract อยู่ ซึ่งโดยปกติจะไม่มีปัญหาเพราะยังติดต่อกันได้ หรืออาจจะใช้ฐาน legitimate interest ได้กรณีที่เป็นลูกค้าเก่าแต่ยัง active คำถามที่ถามมานั้นน่าจะเป็นกรณีลูกค้า non active ที่เว้นระยะมานาน ถ้าเป็นตามลักษณะที่กล่าวมาข้างต้นจะเป็นโจทย์ที่บริษัทจะต้องอธิบายว่าลูกค้าจะคาดหมายได้หรือไม่จากกิจกรรมที่บริษัททำกับลูกค้าอยู่เดิมมีบริบทอะไรที่พอจะบอกได้ว่าลูกค้าสามารถคาดหมายได้ว่าทางบริษัทจะติดต่อไป ในฐานะผู้ให้คำแนะนำขอตอบว่า ถ้าไม่มีหมายความว่าไม่ได้ คือถ้าไม่มีอะไรที่อธิบายได้ จะหมายความว่าไม่ได้ จะต้องเริ่มกระบวนการใหม่ กรณีที่เป็น non active จะเป็นการติดต่อใหม่ แต่ถ้าไม่มีอะไรอยู่เลยก็ต้องขอ consent

นายปริย

จากตอนต้นที่กล่าวว่า เพื่อเป็นการ comply ตามกฎหมาย PDPA นั้น หนึ่งในเรื่องที่จะต้องดำเนินการได้แก่ การแต่งตั้ง DPO (Data Protection Officer) คำถามคือ เนื่องจากธุรกิจในตลาดทุนนั้นมีความหลากหลาย ไม่ว่าจะเป็นเรื่องของประเภทธุรกิจซึ่งแบ่งออกเป็น 14 ประเภท เรื่องขนาดขององค์กรที่มีความต่างกันมาก เช่น บริษัทหลักทรัพย์ บริษัทหลักทรัพย์จัดการลงทุน หรือ LBDU ความสามารถในการที่จะต้อง comply ตามกฎหมายมีความแตกต่างกันอย่างไร ระหว่างบริษัทที่อยู่ในกลุ่มอันดับต้นๆ กลุ่มบริษัทที่มีขนาดเล็กลงมา หรืออาจจะเป็นประเภทธุรกิจที่ไม่ได้ดำเนินการกับลูกค้าที่หลากหลาย ทุกกลุ่มมีจุดตัดอยู่ที่ใด สาเหตุที่ถามถึงความแตกต่างเนื่องจากมีคนตั้งคำถามว่า DPO จำเป็นต้องมีหรือไม่ ส่วนคำถามที่ได้รับเกี่ยวกับ DPO จากบริษัทใหญ่จะเป็นคำถามว่า DPO สามารถมีเป็นองค์คณะได้หรือไม่ ไม่ใช่มี DPO เพียงท่านเดียวแล้วมีคณะทำงานที่ช่วย กล่าวคือ DPO มีความเป็นองค์คณะรับผิดชอบร่วมกันได้หรือไม่

ผศ.ดร. ปิยะบุตร

คำตอบหลักๆคือเป็นองค์คณะได้ แต่เมื่อถึงเวลาปฏิบัติงานจะต้องมีหัวหน้าหรือผู้นำ แม้ DPO จะเป็นองค์คณะก็จะต้องมีผู้นำ เคยมีคำถามว่า DPO มีจำนวนเป็นเลขคู่ได้หรือไม่ กล่าวคือแต่งตั้งให้มี DPO 2 คนแล้วทำงานด้วยกัน คำถามที่ตามมาคือการทำงานจะเป็นรูปแบบใดหากทั้ง 2 คนมีอำนาจเท่ากันแล้วเกิดกรณีมีประเด็น

ความเห็นไม่ตรงกัน งานของ DPO นั้นไม่ควรเป็นงานตีความกฎหมาย ซึ่งขอเน้นย้ำว่างานนี้เป็นงานที่ค่อนไปทาง IT จะไม่เหมือนงานกฎหมายอื่นเพราะปัจจุบันมีการใช้เทคโนโลยีมาก ดังนั้นหากมี DPO 2 คนแล้วจะตีความกฎหมายโดยไม่อ้างอิงมาตรฐาน ISO 27001 หรือ GDPR คนแรกกล่าวว่ากิจกรรมนี้เป็นกิจกรรมที่มีความเสี่ยงสูง ในขณะที่ DPO อีกคนกล่าวว่ากิจกรรมนี้เป็นกิจกรรมที่มีความเสี่ยงกลาง จะกลายเป็นความเสี่ยงต่อองค์กร ดังนั้นงานหลักคือจะต้องอ้างอิงกับมาตรฐาน DPO มีหน้าที่ค้นคว้าว่า ในกรณีแบบนี้จะมีการประเมินว่าเข้ากรณีใดที่มีมาตรฐานรองรับ เข้าใจว่าสิ่งที่กังวลกันคือ บุคลากรในหน่วยงานมองว่าต้องตีความต้องรับผิดชอบเมื่อกล่าวใด ๆ ออกไปและกลัวจะมีความผิด แต่หากมีการอ้างอิงมาตรฐานแล้วกระทำตามนั้นก็จะไม่ใช่สิ่งที่น่ากังวล การปฏิบัติตามที่กล่าวข้างต้นจะไม่ทำให้เกิดปัญหาเรื่องความรับผิดหรือ liability ดังนั้นจึงไม่ใช่สิ่งที่ควรกังวล

นายปริย

ระหว่างบริษัทที่มีขนาดใหญ่ มีธุรกรรมเกี่ยวกับข้อมูลมากกับบริษัทขนาดเล็กจะมีจุดตัดที่ใด ตามความเข้าใจขนาดขององค์กรจะนำไปสู่สิ่งที่บริษัทต้องปฏิบัติใช่หรือไม่ สิ่งที่ต่างกันคืออะไรนอกเหนือจากการมีหรือไม่มี DPO

ผศ.ดร. ปิยะบุตร

การมี DPO มีหลักอยู่ 2 ข้อ ข้อ 1 คือถ้าเป็นองค์กรขนาดเล็ก คณะกรรมการอาจจะยกเว้นไม่ต้องทำบันทึกรายการ ROP และข้อ 2 อาจจะไม่ต้องมี DPO แต่ส่วนที่เป็นหลักการจะต้องเหมือนกัน การใช้สิทธิยังต้องได้เช่นกัน ความแตกต่างขององค์กรขนาดใหญ่และขนาดเล็กนั้น สำหรับองค์กรขนาดใหญ่ตาม PDPA สิ่งแรกจะดูในเชิงบุคลากรขององค์กร กล่าวคือจะต้องเกี่ยวข้องกับจำนวนคนและปริมาณงานที่มาก และสิ่งที่ 2 คือดูตามจำนวนข้อมูล (data) ในที่นี้คือ data ของ data subject นั่นคือตัวบุคคลที่ได้รับผลกระทบจากการทำงาน สมมติว่าบริษัทเป็นองค์กรขนาดไม่ใหญ่ มีพนักงาน 10 คนแต่มีการ process data ของคนหลักหมื่น keyword สำคัญคือ core activity ของธุรกิจนั้นกระทบคนจำนวนมาก เหตุผลพื้นฐานคือกิจการของบริษัทส่งผลกระทบกับคนจำนวนมากหรือไม่ มีความเสี่ยงมากน้อยเพียงใด หลักการจะเป็นเช่นนั้น

สำหรับเส้นที่ขีดกำหนดอย่างไรสุดท้ายคำตอบคือต้องรอคณะกรรมการ หากเทียบเคียงกับ GDPR แล้ว GDPR จะมีเกณฑ์กำหนดชัดเจนคือ 250 คนในการแบ่งขนาดบริษัทใหญ่กับบริษัทเล็ก จำนวน record ก็ไม่มีเกณฑ์กำหนดชัดเจน แต่หากเป็นระดับ 1,000 – 10,000 record บริษัทจะต้องพิจารณาแล้วว่ามาก เมื่อพูดถึงการ

ปฏิบัติตามกฎหมายฉบับนี้ ตามจริงแล้วไม่เชิงเป็นการทำให้แตะเส้น แต่เป็นลักษณะว่าทำอย่างไรจึงจะจัดการความเสี่ยงให้เรียบร้อย การแตะเส้นนั้นเป็นความคิดดั้งเดิมแต่เรื่องนี้เป็นเรื่องของความเสี่ยงดังนั้นความเสี่ยงของหน่วยงานคือ ถ้าเป็นธุรกิจแบบเดียวกันขนาดใกล้เคียงกันแต่กิจกรรมต่างกัน ผู้ประกอบธุรกิจจะประเมินเหมือนกันไม่ได้ด้วยสภาพ ดังนั้นเรื่องนี้เป็นเรื่องเฉพาะ ผู้ประกอบธุรกิจต้องประเมินเองว่าสามารถรับความเสี่ยงได้มากน้อยเพียงใด สำหรับ DPO ในต่างประเทศ สิ่งแรกที่ทำคือ แต่งตั้ง DPO เพราะงานจะไม่มีความคืบหน้าหากไม่มีเจ้าภาพรับผิดชอบ นั่นคือวิธีคิดในต่างประเทศ ดังนั้นหากผู้ประกอบธุรกิจเข้าใจวิธีคิดนี้ก็จะพยายามหาบุคลากรเพื่อมา implement และจัดการความเสี่ยง แต่ไม่ใช่เรื่องที่ว่า ถ้ามีเช่นนี้แต่งตั้งคนนี้แล้วได้ จะเป็นการมองคนละมุมกัน

นายปริย

เนื่องด้วยเรื่องนี้เป็นเรื่องที่ใหม่ ดังนั้นทุกคนจะเดินหน้าไปพร้อมกัน ขอให้อ. ปิยะบุตรแนะนำคุณสมบัติหรือคุณลักษณะของ DPO ที่เหมาะสมว่าควรแต่งตั้งคนที่มีลักษณะใด

ผศ.ดร. ปิยะบุตร

ขอตอบว่าคนที่มีใจ เนื่องจากในด้านความรู้ทุกคนสามารถเรียนทันกันหมด หรือประสบการณ์สำหรับเรื่องนี้ทุกคนก็เริ่มมาในเวลาไล่เลี่ยกัน ที่เป็นปัญหาคือคนที่ไม่ให้ความสำคัญกับเรื่องนี้ แม้อธิบายอย่างไรก็ไม่สามารถดำเนินงานให้ลุล่วงได้

ดร. ไกรพิชิต

เรื่องนี้เป็นปัญหาที่ถกเถียงกันอย่างมากถึงหลักเกณฑ์ในการแต่งตั้ง DPO สำหรับเกณฑ์ของ GDPR คือต้องเป็นบุคคลที่รู้เกี่ยวกับการประมวลผลในองค์กร และขอเน้นย้ำอีกครั้งจากที่อ. ปิยะบุตรกล่าวข้างต้นว่าต้องเป็นคนที่มีใจ กล่าวคือเป็นคนที่เห็นความสำคัญของงานนี้ หากย้อนกลับไปเรื่อง concept แนวคิดจะเป็นเรื่องของ risk management มากกว่า compliance การแตะเส้นเปรียบเสมือนการทำตามกฎหมาย การไม่แตะเส้นจะเป็นการเพิ่มความเสี่ยงซึ่ง DPO จะช่วยในเรื่องนี้ได้มาก ประเด็นที่น่าสนใจของนายปริยคือ ในธุรกิจอุตสาหกรรมเดียวกันมีทั้งผู้ประกอบธุรกิจรายใหญ่และรายเล็ก และเนื่องจากบริษัทจะต้องมีระบบจัดการทำ ROP มี DPO หรือมีระบบ

สารสนเทศ สิ่งเหล่านี้ล้วนเป็นต้นทุนในการทำธุรกิจทั้งสิ้น ขอถามอ. ปิยะบุตรว่าการปฏิบัติตามกฎหมายนี้จะเกิด cost มากน้อยเพียงใดในการ implement เพราะด้วยสภาพการแข่งขันทางด้านธุรกิจ บริษัทใหญ่จะมีต้นทุนและความพร้อมมากกว่าและนำไปสู่การแย่งลูกค้าบริษัทเล็ก ทำให้บริษัทเล็กมองว่าการปฏิบัติตามกฎหมายนี้ทำให้เสียเปรียบในการแข่งขัน ขอให้อ. ปริยะบุตรช่วยชี้แจงในเรื่องนี้

ผศ.ดร. ปิยะบุตร

เป็นเรื่องของการจัดการความเสี่ยงซึ่งขึ้นอยู่กับความเสี่ยงที่ผู้ประกอบธุรกิจประเมินตัวเองเป็นหลัก หากเป็นองค์กรขนาดเล็กอาจจะใช้เพียง excel ธรรมดาไม่มีระบบ ERP ที่ต้องดูแล เพราะฉะนั้นจะไม่พบปัญหาเรื่องของ solution การใช้ software ที่มีราคาแพงโดยอัตโนมัติ ขณะเดียวกันจำนวนลูกค้าก็จะมีไม่มาก ทำให้ไม่ต้องจัดทำกระบวนการรองรับทำ Consent Management ทำ Data Subject Request Management ที่เป็นระบบ กล่าวคือใช้อีเมล์ธรรมดาก็สามารถดำเนินการได้ ซึ่งไม่ควรนำไปเทียบกับบริษัทอื่นที่มี software และต้องเสียค่าใช้จ่ายเป็นหลักล้านต่อปี หลักปฏิบัติคือบริษัทจะต้องทำอย่างไรเพื่อบริหารความเสี่ยงขององค์กรซึ่งจะเหมาะสมด้วยสภาพของเรื่องอยู่แล้ว ไม่ใช่ว่าอยู่ๆผู้ประกอบธุรกิจจะยอมจ่ายเงินราคาแพงเพื่อทำในสิ่งที่ไม่ใช่ ดังนั้นเรื่องต้นทุนไม่ใช่ปัจจัยที่จะทำให้บริษัทเล็กมีความเสียเปรียบ ถ้าเป็นกรณีรายย่อยมากๆ ทำงานอยู่คนเดียว และไม่ได้เก็บ record ไว้ คือสั่งสินค้ามาแล้วก็ส่งไป ข้อมูลทกุอย่างอยู่ใน Shoppee หรือ Lazada แล้วผู้ประกอบการไม่ได้ดึงข้อมูลจากระบบนั้นออกมาเก็บ ซึ่งโดยปกติ Shoppee และ Lazada จะมี privacy policy อยู่แล้ว กรณีดังกล่าวถ้าผู้ประกอบการไม่ได้ทำอะไรเกี่ยวกับข้อมูล เพียงประกาศว่าร้านค้าของท่านไม่ได้เก็บข้อมูลเหล่านี้ ก็ไม่ต้องทำอะไรและไม่มีความรับผิดชอบใดเลย อย่างไรก็ตามไม่ใช่ว่ามาตรวจพบภายหลังว่ามีการเก็บข้อมมูลไว้ ประเด็นปัญหาคือผู้ประกอบการมักจะมีแนวคิดว่าต้องการจะทำอย่างอื่นแล้วพยายามหลบหลีก การกระทำเช่นนี้จะทำให้เรื่องก็จะยุ่งยากมากขึ้น

ดร. ไกรพิชิต

สรุปคือตรงไปตรงมา ธุรกิจเล็กสามารถใช้วิธีการอื่นไม่จำเป็นต้องแบกรับภาระเรื่องต้นทุนทางด้านระบบสารสนเทศหรือระบบที่เกี่ยวกับการจัดการข้อมูลส่วนบุคคลขนาดใหญ่โดยการใช้ excel ธรรมดาหรือจัดสรรเจ้าหน้าที่ในการรับเรื่องร้องเรียนหรือทำการจัดการข้อมูลลูกค้า/ข้อมูลส่วนบุคคลของลูกค้า กล่าวคือทำตามกำลังที่สามารถจะทำได้และเหมาะสมกับธุรกิจขององค์กรนั้น ๆ

อีกหนึ่งประเด็นคำถามที่น่าสนใจจากธุรกิจด้านการขายผลิตภัณฑ์การลงทุน ซึ่งก่อนหน้านี้อ. ปิยะบุตรได้อธิบายเกี่ยวกับเรื่อง KYC/CDD ในเรื่อง sensitive data ของการรู้จักลูกค้าของบริษัทเองไปแล้วนั้น มีคำถามเพิ่มเติมว่า รูปถ่ายของลูกค้าที่นำมาเป็นส่วนหนึ่งในการทำ KYC/CDD เป็น sensitive data หรือไม่ และประวัติทางด้านกฎหมายการฟอกเงินของลูกค้าว่าเคยกระทำความผิดในกฎหมายฟอกเงินหรือเปล่า เรื่องนี้ถือเป็น sensitive data หรือไม่ เนื่องจากบริษัทที่ทำการขายผลิตภัณฑ์การลงทุนอาจจะต้องทำ Due Diligence ของลูกค้า นอกจากนี้การทำความรู้จักลูกค้ามากขึ้นด้วยการหาข้อมูลบน Google website เพื่อให้ได้ข้อมูลสาธารณะเกี่ยวกับตัวลูกค้า หรือแม้กระทั่งการเก็บข่าวในทางไม่ดีเกี่ยวกับลูกค้าเพื่อประเมินความเสี่ยง จะเป็นไปตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่ และมีคำแนะนำอย่างไรในการบริหารจัดการข้อมูลเหล่านี้

<u>ผศ.ดร. ปิยะบุตร</u>

มีข้อสังเกตว่า คำถามที่ผู้ประกอบการถามในปีนี้จะเป็นคำถามที่มีการพัฒนาและลงรายละเอียดในกิจกรรมมากขึ้น สำหรับคำถามนี้ ขอให้ย้อนกลับไปที่หลักการเดิมคือ PDPA ไม่ได้เปลี่ยนแปลงสิ่งที่ผู้ประกอบธุรกิจกำลังดำเนินการอยู่ เมื่อก่อนผู้ประกอบธุรกิจเคยทำได้ ปัจจุบันก็จะยังคงทำได้ต่อไป แต่จะต้องชี้แจงว่าการกระทำเช่นนี้จะเข้าฐานการประมวลผลใด หากสามารถทำได้จะไม่มีปัญหาก็เพียงแจ้งลูกค้าไปตามมาตรา 23 ที่นายกำพลได้อธิบายไปแล้วก่อนหน้า ประเด็นคำถามน่าจะเกิดจากความกังวลหรือไม่แน่ใจว่าสิ่งที่ทำจะถูกต้องหรือไม่ สิ่งสำคัญคือ ไม่เคยมีการแจ้งมาก่อนมากกว่า หากผู้ประกอบธุรกิจแจ้งลูกค้าอย่างชัดเจนว่ากิจกรรมใดบ้าง พ.ร.บ. PDPA เป็นตัวกำหนดให้ผู้ประกอบการชี้แจ้งให้ data subject รู้ เพราะฉะนั้นการตรวจสอบประวัติอาชญากรรมมีเหตุผลที่ผู้ประกอบธุรกิจต้องตรวจก็สามารถชี้แจงให้ทราบว่าจะต้องตรวจ คำถามที่ว่าเป็น sensitive data หรือไม่ เรื่องประวัติอาชญากรรมด้วยนิยามนั้นเป็นอยู่แล้ว

สำหรับรูปถ่าย เนื่องจากที่ถามมาเป็นการกล่าวรวมๆว่ารูปถ่าย จึงไม่ทราบแน่ชัดว่ารูปถ่ายในระบบถูกเก็บในลักษณะใด แต่หากไม่มีการ process คือเมื่อเห็นรูปหรือเอกสารฉบับนี้แล้วสามารถรู้ได้ว่าเป็นของใครกรณีนี้จะไม่เป็น sensitive data แต่ถ้ามีการ process หรือมีคำอธิบายประกอบว่ารูปนี้คือใครจะถือเป็น sensitive data

<u>นายกำพล</u>

เมื่อเป็น sensitive data จะนำไปสู่การเลือกปฏิบัติในการใช้บริการหรือไม่ แต่บางกรณีเช่น User authentication ธรรมดา กรณีนี้อาจจะไม่เป็น

ผศ.ดร. ปิยะบุตร

นั่นจึงเป็นเหตุผลสำคัญที่ทำให้มีมาตรา 26 เพื่อป้องกันไม่ให้เกิดการเลือกปฏิบัติ สำหรับเรื่องฐานการประมวลผล เท่าที่เข้าใจคือมีคำอธิบายความจำเป็นประกอบฐานอยู่แล้วแต่ไม่เคยมีการถูกแจ้งให้เป็นที่เรียบร้อย การแจ้งคือจะต้องแจ้งบอกว่าฐานอะไรตามประกาศใด ซึ่งถ้ามีขั้นตอนเรียบร้อยทุกอย่างจะไม่มีปัญหาและทุกคนจะสบายใจ จากประสบการณ์ที่เคยเจอ ตัวอย่างเช่น มีการขอให้ส่งข้อมูลแต่ regulator ไม่เคยมีประกาศ กล่าวคือไม่เคยมีความชัดเจนว่าจะต้องส่งข้อมูลแต่ว่ามีการส่งข้อมูลดังกล่าวในชีวิตจริง เป็นต้น กรณีเช่นนี้ regulator ต้องทำให้มีความชัดเจนว่าต้องการข้อมูลนี้เพื่อตอบโจทย์ใดที่เป็นความจำเป็นตามการกำกับดูแล ถ้าไม่เคยมีกำหนดมาก่อนก็ต้องช่วยออกประกาศให้ชัดเจนเรียบร้อย

นายปริย

มีประเด็นต่อเนื่องจากของอ. ปิยะบุตร คือเรื่องที่บอกว่า regulator ขอข้อมูล หากนำมาประยุกต์กับเรื่องการเปิดบัญชีซื้อขายหลักทรัพย์หรือว่าหน่วยลงทุนในตลาดทุน ตอนนี้ทางสำนักงานก.ล.ต. ได้พัฒนา single form ขึ้นมาเพื่ออำนวยความสะดวกให้กับผู้ลงทุนเวลาไปเปิดบัญชีซื้อขาย ซึ่งข้อมูลที่ให้นั้นจะเป็นมาตรฐานที่ภาคอุตสาหกรรมสามารถใช้ได้ทุกบริษัท นี่คือสิ่งที่ทางสำนักงานก.ล.ต. วางแผนจะเริ่มใช้ในปีหน้า การทำ single form ทางสำนักงานเองจะหารือกับภาคอุตสาหกรรมและดำเนินการไปด้วยกัน โดยเน้นที่สำนักงานก.ล.ต. ต้องการให้บริษัทหลักทรัพย์ใช้ในการเก็บข้อมูล KYC/CDD ของลูกค้า ซึ่งทางก.ล.ต. เองพยายามจะอำนวยความสะดวกให้จึงออกมาเป็นในรูปแบบของ single form เมื่อลูกค้าไปเปิดบัญชีก็จะต้องให้ข้อมูลต่าง ๆ หากอ้างอิงตามอ.ปิยะบุตรอธิบายคือ การที่ regulator ประกาศว่าข้อมูลเหล่านี้เป็นข้อมูลจำเป็นสำหรับบริษัทหลักทรัพย์ที่จะรับลูกค้านำไปใช้ในการประมวลผลโดยมีที่มาจาก regulation เพราะฉะนั้นสามารถตีความได้ว่า single form มีที่มาเช่นนี้และไม่ต้องขอ consent ของลูกค้าใช่หรือไม่

ผศ.ดร. ปิยะบุตร

ใช่ ยกเว้นสำนักงานก.ล.ต. ต้องการ sensitive data สมมติกรณีที่ก.ล.ต. ต้องการข้อมูล sensitive data ใน single form ที่ สำนักงานฯจะเป็นผู้เก็บรวบรวมเอง อาจจะมี 2 ทางออกคือ กรณีที่เป็นงานแบบหลักทรัพย์คือต้องขอความยินยอมก็ถือเป็นเงื่อนไขของการกำกับดูแลได้ อีกกรณีคือ ไปเข้า public task คือสำนักงานก.ล.ต. ระบุว่าเรื่องนี้สำคัญไม่ต้องขอความยินยอม คือพอเป็นแบบฟอร์มเลยต้องขอความยินยอมก่อน เพราะฉะนั้นขอความยินยอมจะง่ายกว่า แต่ถ้าหากเป็นเรื่องอื่นที่ไม่ต้องขอไม่ต้องให้ลูกค้ากรอก ก็จะมีข้อที่เป็นประโยชน์

สาธารณะที่สำคัญ ก.ล.ต. อาจจะต้องมีประกาศเพื่ออธิบายว่าเหตุใดข้อมูลนี้จึงสำคัญ การทำเช่นนี้ทำให้สามารถทำงานได้และทุกคนสบายใจไม่มีปัญหา

นายปริย

กรณีถ้าเป็นข้อมูลจำเป็นเกี่ยวกับการ comply ตามกฎหมายฟอกเงินที่ระบุว่าลูกค้าเคยมีประวัติเกี่ยวกับเรื่องกฎหมายฟอกเงินหรือไม่ ซึ่งจะเป็นส่วนหนึ่งที่ผู้ประกอบการต้องมีการตรวจสอบ กรณีนี้เป็นเรื่องของ sensitive data หรืออ.ปิยะบุตรมองว่าเป็นสิ่งที่อ้างอิงจาก regulation ที่จำเป็นจะต้องขี้แจ้งว่าเป็นข้อมูลที่จะต้องเก็บเพื่อจะให้บริการกับลูกค้า

ผศ.ดร. ปิยะบุตร

หากเป็นไปตามกฎของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ที่สั่งให้เก็บ สำนักงานก.ล.ต. สามารถอ้างได้เลยว่าเป็นสิ่งที่เป็นข้อกำหนด แต่ว่าเมื่อสักครู่ที่อธิบายว่าต้องขอ consent หรือไม่ คือเมื่อระบุว่าเป็นข้อกำหนดมันจะเป็นอีกขั้นหนึ่ง กล่าวคือถ้าลูกค้าไม่ให้ข้อมูลก็จะไม่สามารถทำงานต่อได้ เพราะปปง. กำหนดว่าต้องใช้ เนื่องจากกรณีนี้เป็น sensitive data แต่สำหรับกรณีทั่วไปข้อมูลส่วนบุคคลทั่วไปจะไม่มีประเด็น

ดร. ไกรพิชิต

โดยสรุปคือ แม้เป็นข้อมูล sensitive data แต่ถ้าจำเป็นต้องใช้ในการประกอบธุรกิจก็สามารถขอได้หรือไปหามาได้จากแหล่งข้อมูลที่เป็น public แต่ว่าต้องแจ้งเจ้าของข้อมูล เพราะฉะนั้นกฎหมายพ.ร.บ. ฉบับนี้เปรียบเสมือนการเน้นย้ำสิทธิของเจ้าของข้อมูลส่วนบุคคลอีกครั้ง เรื่องสิทธิในการรับรู้หรือว่าข้อมูลถูกนำไปใช้ทำอะไร ซึ่งเรื่องนี้สำคัญมาก

นายปริย

ที่อ. ปิยะบุตรกล่าวว่าต้องแจ้ง คือแจ้งอยู่ที่ privacy policy ใช่หรือไม่

ผศ.ดร. ปิยะบุตร

ใช่ หลัก ๆ คือ privacy policy ซึ่งในทางปฏิบัติควรจะเขียน privacy policy ให้เสร็จเรียบร้อยเพื่อที่จะไม่ต้องทำงานซับซ้อนหลายชั้น ถึงเวลาที่ลูกค้ามาสมัครกรอกแบบฟอร์ม เมื่อลูกค้าเห็น privacy policy ก็จะรับทราบทุกอย่างที่เราจะทำ แต่ถ้ากรณีที่ทำไม่เรียบร้อย มีสิ่งที่เพิ่มเติมในภายหลัง จะต้องขอเพิ่ม เรามีหน้าที่ต้องทำ notice เพิ่มซึ่งจะเป็นการเพิ่มขั้นตอน ดังนั้นในทางปฏิบัติควรทำให้เสร็จเรียบร้อยตั้งแต่แรก

นายปริย

การแจ้งให้ลูกค้าทราบอาจจะเป็นไปในลักษณะการโพสต์ไว้บน website ก็ได้ใช่หรือไม่ หากลูกค้าสนใจเข้าไปดู หรือขอบริการก็สามารถอ่านได้บน website

ผศ.ดร. ปิยะบุตร

ทำได้หลายวิธีการ เช่น อาจจะมี QR code สำหรับผู้ที่มาสมัครงานเพื่อเข้าไปดู privacy policy ได้ตามที่แจ้งไว้ แต่ทั้งนี้จะต้องมีวิธีที่ทำให้เจ้าของข้อมูลสามารถเข้าถึงได้ ว่าต้องไปดูที่ใด

นายปริย

กรณีเป็นตัวแทนขายสังกัดบริษัทหลักทรัพย์หรือธนาคาร เวลาไปพบลูกค้าจะต้องมีวิธีการให้ลูกค้าทราบ privacy policy ก่อนเช่นกันใช่หรือไม่

ผศ.ดร. ปิยะบุตร

ใช่ หากเป็นตัวแทนสามารถเอาของบริษัทให้ลูกค้าดู หรือแจ้งลูกค้าว่าสามารถดูได้พร้อมแจ้งวิธี เช่น มี QR code หรือเอกสารแนบให้

นายปริย

เพราะฉะนั้นสำหรับกลุ่มตัวแทนขาย ในการอบรมหรือว่าให้ใบอนุญาต (license) เกี่ยวกับผู้ให้คำแนะนำผู้ลงทุน อาจจะต้องมีการรวมหลักสูตรความรู้เกี่ยวกับ PDPA เข้าไปด้วย เพราะกลุ่มคนเหล่านี้จะต้องติดต่อผู้ลงทุนโดยตรงค่อนข้างมาก สิ่งนี้น่าจะเป็นจุดที่สำคัญ

ดร. ไกรพิชิต

เป็นส่วนหนึ่งในหน้าที่ที่ทางสำนักงานก.ล.ต. จะต้องส่งเสริมมากขึ้น ขณะนี้ทางก.ล.ต. ได้รายละเอียดความชัดเจนในเรื่องที่เกี่ยวกับการ touch ลูกค้ามากพอสมควรแล้ว ขอเริ่มคำถามในกลุ่มที่ 2 ของภาคธุรกิจที่เป็นของกลุ่มธุรกิจตัวกลางหลักทรัพย์และบริษัทหลักทรัพย์จัดการการลงทุน ประเด็นคำถามที่น่าสนใจคือ ในขณะที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลยังไม่มีการกำหนดรายละเอียด โดยเฉพาะอย่างยิ่งเรื่องการตีความฐานะคู่สัญญา และหลายๆงานในธุรกิจที่เป็นกระบวนการต่อเนื่องกัน เช่น กระบวนการซื้อขายหลักทรัพย์จะต้องมีการส่งข้อมูลลูกค้าไปยังหน่วยงานต่าง ๆ เริ่มตั้งแต่บล. ที่เป็นคนรับลูกค้า เมื่อมีการรับคำสั่งซื้อขายแล้วก็นำส่งคำสั่งซื้อขายเข้าสู่ระบบการซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์แห่งประเทศไทย มีการ clearing การจดทะเบียน การทำ settlement การบันทึกว่าใครเป็นเจ้าของที่ราคาใด ผ่านระบบที่หลากหลายไม่ว่าจะเป็น SET, TSD, TCH, Finnet, Registart หรือแม้แต่ custodian ซึ่งในการทำ 1 activity ต้องผ่านหลาย agent หลายองค์กรมาก ประเด็นข้อสงสัยคือ หากใน 1 activity มีความซับซ้อนเกี่ยวเนื่องกันหลายองค์กร data controller หรือ data processor คือใครและ ควรทำอย่างไรเนื่องจาก ผู้ที่ทำหน้า data controller จะต้องแจ้งรวมถึงจัดการข้อมูลส่วนบุคคลของลูกค้าค่อนข้างมาก และ data processor จะต้องมีข้อตกลงกับ data controller ในการ process ข้อมูล เพราะฉะนั้นการแบ่งหน้าที่ให้ชัดเจนมีความสำคัญอย่างยิ่ง โดยเฉพาะในสายธุรกิจที่มีความต่อเนื่องและเกี่ยวพันกับหลายองค์กร ขอถามอ. ปิยะบุตรว่าแนวคิดในการกำหนด data controller และ data processor อย่างไร หรือจะทำอย่างไรให้ภาคธุรกิจมีความชัดเจนมากขึ้นในการ comply ตามพ.ร.บ. PDPA

ผศ.ดร. ปิยะบุตร

ข้อนี้เป็นคำถามที่สำคัญเนื่องจากมีความเข้าใจคลาดเคลื่อนกันอยู่ในเรื่องนี้ เรื่องแรกขอยกตัวอย่างที่ไม่ได้เกิดขึ้นจริงว่า สำนักงานก.ล.ต. สามารถไปตั้งใครเป็น controller และ processor ในหน่วยงานได้หรือไม่ ตามนิยามความหมายของ controller คือคนที่มีอำนาจตัดสินใจทำอะไรต่อข้อมูลส่วนบุคคลด้วยตนเองเพื่อประโยชน์ของตนเอง และ processor คือคนที่ทำงานประมวลผลข้อมูลตามคำสั่งของ controller หาก controller ไม่สั่งจะไม่สามารถทำได้ ความหมายนั้นค่อนข้างเรียบง่ายและเข้าใจง่าย ประเด็นคือเรื่องนี้เป็นเรื่องที่ดูตามความเป็นจริงตามภาษากฎหมายเรียกว่า de facto คือทุกอย่างดูตามที่เกิดขึ้นจริง แม้จะมีสัญญาระบุว่าเป็น processor แต่จริง ๆ แล้วเป็น controller ก็สามารถเป็น controller ได้ เพราะฉะนั้นจึงไม่ใช่ประเด็นที่จะไปกำหนดอะไรต่อใคร แต่ถามว่ากำหนดได้หรือไม่ คำตอบคือได้ เดิมเป็น controller อยากจะเป็น processor ก็จะต้องเปลี่ยนวิธีการทำงานให้ตนเองเป็น processor

เมื่อพูดถึง activity ที่ต่อเนื่องกันไป ยกตัวอย่างแรก คือแต่ละ entity ทำงานด้วยตัวของเขาเอง แต่ละส่วนทำงานด้วยตัวเองไม่ได้ขึ้นต่อกันแต่ข้อมูลถูกส่งมาเป็นทอดๆและทำงานของตัวเองเป็นทอดๆ กรณีนี้ทุกคนเป็น controller คือไม่ได้มีประเด็นว่าใครเป็น processor ให้ใคร ตัวอย่างง่ายๆเช่น ถ้าเป็นผู้ให้บริการ payment แล้วร้านค้ามาใช้บริการ payment คนทำ payment ก็จะทำกิจกรรม payment ของตนเอง ไม่ได้ช่วยขายของ คือให้บริการ payment เก็บค่าธรรมเนียมจากการทำ payment กรณีเช่นนี้คือจะเป็น controller ด้วยตัวของเขาเอง เพียงแค่นำข้อมูลนั้นมาทำ payment ซึ่งเป็นการให้บริการไปที่ร้านค้าด้วย ตัวอย่างต่อมาคือ การส่งไปรษณีย์หรือพัสดุ การเอาของไปส่งไปรษณีย์หรือส่งพัสดุ ไม่ได้ทำให้ไปรษณีย์เป็น processor ให้ผู้ใช้บริการ เพราะไปรษณีย์นั้นมีบริการส่งพัสดุอยู่แล้ว ข้อมูลที่ผู้ใช้บริการส่งไปคือฉลากหน้ากล่อง ข้อมูลนั้นคือข้อมูลที่ไปรษณีย์ใช้ซึ่งใช้ด้วยตนเอง ไม่ได้ process content ข้างในพัสดุหรือไปรษณีย์ให้ผู้ใช้บริการ เจ้าของพัสดุไปรษณีย์ยังคงเป็น controller ในส่วนของ content ข้างในไปรษณีย์หรือพัสดุเช่นเดิม อีกตัวอย่างที่ได้รับคำถามมา คือ โทรศัพท์มือถือ การใช้งานสื่อสารด้วยโทรศัพท์มือถือ ผู้ให้บริการโทรศัพท์มือถือจะเป็น processor ให้กับผู้ใช้บริการหรือไม่ คำตอบคือไม่ ผู้ให้บริการโทรศัพท์มือถือนั้นให้บริการด้วยตัวของเขาเอง ไม่ได้มาทำงานให้กับผู้ใช้บริการ สิ่งที่ผู้ใช้บริการส่งไปคือเพื่อประโยชน์ในการให้บริการโทรศัพท์มือถือเท่านั้น ไม่ได้สั่งให้ผู้ให้บริการทำงานให้เพราะมีการจ่ายค่าบริการด้วย คำอธิบายเรื่องนี้อยากให้เปรียบเทียบไปที่ระบบ outsource คือเวลาใช้งาน outsource แล้ว outsource ทำงานให้เราเต็มที่แบบ turnkey กรณีนี้จะเป็น processor ตัวอย่างถัดมาคือถ้ามีข้อมูลไหลมาเป็นท่อนๆ และแต่ละท่อนทำงานตามคำสั่ง ตัวอย่างเช่น สำนักงานก.ล.ต. outsource ที่ปรึกษา IT เจ้าใหญ่เจ้าหนึ่ง ซึ่งเจ้านี้ทำงานทุกอย่างตามคำสั่งก.ล.ต. คือมี TOR และทำทุกอย่างตาม TOR ต่อมา outsource เจ้านี้ไป sub contract กับอีกบริษัทหนึ่งและทำตาม TOR นี้หมด ทุกอย่างเป็นเช่นนี้ตลอดทั้งสาย นั่นคือกลุ่มนี้จะเป็นทั้ง processor และ sub processor ให้กับก.ล.ต. ที่เป็น controller ทั้งหมด จะแตกต่างกับ

งานไปรษณีย์และงาน payment หรือโทรศัพท์มือถือที่ต่างคนต่างทำงานตามหน้าที่ของตัวเอง ไม่ได้มาทำงานตามคำสั่ง

กลุ่มที่น่าสนในคือกลุ่มที่ทำงานตามวิชาชีพ ได้แก่ ผู้สอบบัญชีหรือผู้ที่เป็น auditor ซึ่งกลุ่มคนเหล่านี้มีหลายกิจกรรมที่ทำอยู่ หากกิจกรรมนั้นเป็นกิจกรรมในเชิงวิชาชีพ เราไปสั่งเขาไม่ได้เพราะมีวิชาชีพค้ำอยู่ คนกลุ่มนี้จะต้องทำการประมวล ตรวจสอบข้อมูลตามวิชาชีพ ซึ่งมีกรอบมี framework ที่ชัดเจน กรณีนี้จะเป็น controller แต่หากงานที่ให้คนกลุ่มนี้ทำเป็นการ consult หรือให้บริการตาม TOR ที่ระบุทุกอย่างหรือทำตามคำสั่ง เช่นนี้จึงจะเรียกว่าเป็น processor อย่างตัวอาจารย์เองในด้านกฎหมาย ถ้าเป็นที่ปรึกษากฎหมาย ให้คำปรึกษาทางกฎหมาย โดยสภาพคำปรึกษาทางกฎหมายคือนำวิชาชีพมาให้ความเห็น เพราะฉะนั้นตัวอาจารย์จะเป็นคนพูดเองว่า ควรจะเห็นข้อมูลอะไร ควรเอาข้อมูลใดมาดู จะไม่ได้ทำตามคำสั่ง แต่ถ้ากลับกัน สมมติว่าสำนักงานก.ล.ต. บอกว่าให้ดูข้อมูลเท่านี้แล้วให้ความเห็น จะต้องบอกว่าไม่ได้ ตัวอาจารย์ดูเช่นนี้ไม่ได้ไม่เพียงพอ ต้องขอดูสิ่งอื่นเพิ่ม

นายปริย

จากที่อ. ปิยะบุตรอธิบายข้างต้นว่าเมื่อใดจึงจะเป็น role controller เมื่อใดจึงจะเป็น role processor การ comply ตามกฎหมาย PDPA นั้นจะต้องมีสัญญาหรือข้อตกลงอะไรหรือไม่เพื่อที่จะแสดงให้เห็นผู้ใดอยู่ในบทบาทหน้าที่ใด

ผศ.ดร. ปิยะบุตร

ใช่ ในกฎหมายจะระบุไว้ว่า ความสัมพันธ์ระหว่าง controller กับ processor จะต้องมีข้อตกลงระหว่างกันอย่างชัดเจน ประเด็นของกฎหมายคือ ให้ controller สามารถบังคับ processor ได้ ซึ่งถ้าไม่มีสัญญาอาจจะเกิดปัญหาได้ โดยปกติสัญญาหรือ Service agreement นั้นมีอยู่แล้ว แต่ไม่มีเนื้อหาเกี่ยวกับการทำ processing กฎหมายเลยระบุว่าให้สัญญานั้นกล่าวถึงเรื่อง processing ด้วย และจะต้องทำหน้าที่ตามที่กฎหมายกำหนด ดังนั้นตามความหมายคือจะได้มีการบังคับกันได้ กฎหมายต้องการสิ่งนี้

นายกำพล

ในพระราชกฤษฎีกาในมาตรา 3 ที่มีการประกาศเลื่อนการบังคับใช้ไปอีก 1 ปี ย่อหน้าที่ 2 พูดถึงเฉพาะผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้นไม่ได้พูดถึงผู้ประมวลผลข้อมูล สัญญานี้จะสามารถใช้เพื่อขยายผลต่อได้หรือไม่

ผศ.ดร. ปิยะบุตร

ใช่ ด้วยหลักการไม่ควรจะมี processor โดยที่ไม่มี controller เพราะว่า processor คือ outsource ของ controller และควรจะเป็นเช่นนั้น คือตอนนี้ยังไม่เห็นตัวอย่างที่จะเกิดเหตุการณ์แบบนั้นขึ้นได้ แต่มีคนทักมาแล้วเหมือนกันว่าพระราชกฤษฎีการะบุเฉพาะผู้ควบคุม แล้วผู้ประมวลผลจะมีปัญหาหรือไม่ คำตอบคือต้องไม่มีเพราะ processor ต้องขึ้นกับ controller แต่หากมีเหตุการณ์เป็นอย่างอื่นก็ต้องมาดูรายละเอียดว่าเหตุการณ์นี้คืออะไร

นายกำพล

สิ่งที่เป็นกังวลคือ สมมติว่าหลายองค์กรมีการทำไปแล้ว กำหนดผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูลและมีสัญญาเรียบร้อย การเลื่อนให้เฉพาะผู้ควบคุมแต่ไม่ได้ระบุอย่างชัดเจนว่าผู้ประมวลผลนั้นถูกเลื่อนตามไปด้วย และยังคงเป็นสัญญาเดิม เลยมองว่าน่าจะไปทั้งหมดแม้ว่าสัญญาจะทำขึ้นก่อนหน้าพระราชกฤษฎีกาก็ตาม

ผศ.ดร. ปิยะบุตร

ต้องอ่านตามที่นายกำพลอธิบาย คือดูตามเจตนา หากยกเฉพาะ controller แต่ไม่ยกให้ processor จะต้องมีปัญหาตามมาแน่นอน

ดร. ไกรพิชิต

มีความชัดเจนว่าเป็นการบังคับใช้กับ processor โดยปริยาย เชื่อว่าหลายธุรกิจที่ต้องทำกระบวนการที่ซับซ้อนต่อเนื่องกันจะได้แนวคิดเรื่อง data controller และ data processor รวมถึงนำไปปรับใช้ อีกหนึ่ง

กิจกรรมหลักที่เกิดขึ้นในตลาดทุนคือกิจกรรมในการทำ IPO (Initial Public Offering) ทั้งในหลักทรัพย์และหน่วยลงทุน ซึ่งเป็นกิจกรรมที่เกี่ยวข้องกับการขายหลักทรัพย์ต่อสาธารณะครั้งแรก เข้าใจว่าในการขายหลักทรัพย์ต่อสาธารณะครั้งแรกมีความจำเป็นต้องทำ Privacy notice ด้วย คำถามจากภาคอุตสาหกรรมคือ หากผู้ระดมทุนหรือ Issuer ระดมทุนในหลักทรัพย์หรือแม้กระทั่งบลจ. ซึ่งเป็นผู้ระดมทุนในกรณีของกองทุนรวมต้องการทำ IPO ควรจะแจ้ง Privacy notice ในเอกสารการจองซื้อหรือหนังสือชี้ชวนหรือเอกสารอื่นหรือกำหนดให้แสดงในเวบไซต์ของบริษัทจึงจะเหมาะสม และหากเป็นกองทุนรวม การแจ้ง Privacy notice หน้าที่นี้เป็นของบลจ. เพียงอย่างเดียว หรือกองทุนจำเป็นต้องแจ้งด้วยเช่นกัน เพราะว่ากองทุน บลจ. เป็นคนควบคุมกองทุนรวมอีกครั้งหนึ่ง เพราะฉะนั้นจะเป็นเรื่องของ Privacy notice ว่าต้องแจ้งเมื่อไหร่ แจ้งอย่างไรและใครเป็นผู้แจ้ง

ผศ.ดร. ปิยะบุตร

อยากให้สังเกตว่าคำถามจะเริ่มลงในกิจกรรมเฉพาะเจาะจงซึ่งถือเป็นสัญญาณที่ดีมาก หลักการคือควรจะแจ้งครั้งแรกที่เริ่มเก็บรวบรวมข้อมูลส่วนบุคคล อาจจะต้องถามว่าครั้งแรกที่มีการเก็บคือหนังสือชี้ชวนหรือหนังสือจองซื้อหรือขั้นตอนใด ถ้าในขั้นตอนหนังสือชี้ชวนเริ่มมีการเก็บข้อมูลควรจะต้องแจ้งตั้งแต่ตอนนั้น เพื่อให้ทราบว่ามันจะมีในขั้นตอนนี้ และควรจะเล่าไปตลอดทั้งกระบวนการว่าแต่ละขั้นตอนจะเกิดอะไรขึ้นหลังจากนี้ด้วย ดังนั้นในโอกาสแรกที่มีการเก็บข้อมูลลูกค้า ควรจะเริ่มเลย

ดร. ไกรพิชิต

ขอถามต่อเนื่องเกี่ยวกับเรื่องของ marketing การขาย มีคำถามจากภาคธุรกิจว่าการให้นามบัตรเพื่อการติดต่อธุรกิจถือเป็นการให้ความยินยอม (consent) โดยปริยายหรือไม่ แล้วบริษัทสามารถนำข้อมูลไปติดต่อเพื่อนำเสนอผลิตภัณฑ์และบริการต่าง ๆ ได้หรือไม่ นอกจากนี้หากบริษัทเก็บข้อมูลในการติดต่อลูกค้าที่เป็น prospect มาจากแหล่งอื่นที่ไม่ใช่ลูกค้าของตัวเองโดยตรง บริษัทสามารถโทรไปติดต่อและขอ consent ภายในการโทรติดต่อครั้งแรกได้หรือไม่

ผศ.ดร. ปิยะบุตร

คำถามนี้เป็นตัวอย่างของคำถามที่ไม่ได้ลงกิจกรรม กรณีนี้ไม่ได้ระบุว่านามบัตรนั้นได้มาในกิจกรรมใด บริบทใดเพราะนามบัตรไม่ได้อยู่เพียงบริบทเดียวกิจกรรมเดียว นามบัตรสามารถมาได้หลายลักษณะ โดยธรรมชาติส่วนใหญ่จะเป็นกรณีพบปะกันในทางธุรกิจ แล้วมีการแลกนามบัตรกัน เป็นที่ทราบว่ากรณีเช่นนี้วัตถุประสงค์คือเพื่อให้ติดต่อทางธุรกิจ ไม่ได้เอาไปให้ใช้ทำอย่างอื่น ประเด็นคือ หากใช้นามบัตรเพื่อติดต่อในทางธุรกิจก็จะไม่มีประเด็นต้องขอ consent ซึ่งในลักษณะนั้น อาจอ้างอิงฐาน legitimate interest ประกอบด้วยเพราะเป็นสิ่งที่เกิดขึ้นและสามารถคาดหมายได้ ประเด็นคือ มีการทำ filing เพื่อใช้ในงานที่ติดต่อกันเท่านั้น แต่หากนามบัตรนั้นได้มาในลักษณะอื่น เช่น หย่อนลงไปไว้ในตู้ทั่วไป กรณีนี้จะกล่าวอ้างว่าเจ้าของนามบัตรยินดีที่จะให้นำนามบัตรนั้นไปใช้เพื่อติดต่อกิจกรรมอย่างอื่นซึ่งจะบอกว่าเจ้าของนามบัตรคาดหมายได้นั้นไม่ได้

ดร. ไกรพิชิต

อย่างเช่นตอนนี้มีหลายงานนิทรรศการใช้วิธีการหย่อนนามบัตรแทนทีจะมีการลงทะเบียนโดยตรง เพราะฉะนั้นข้อมูลที่ได้จากนามบัตร เราสามารถไปติดต่อเพื่อเสนอผลิตภัณฑ์ใหม่ ๆ โดยที่ไม่ได้แจ้งเจ้าของนามบัตรล่วงหน้าได้หรือไม่

ผศ.ดร. ปิยะบุตร

จะมีปัญหาว่าเจ้าของนามบัตรไม่อาจคาดหมายได้ ดังนั้นสำหรับกิจกรรมที่ได้นามบัตรมา หากอยากได้อะไรควรจะพูดออกไปตรงนั้นเลย ต้องบอกให้ชัดเจนว่าอยากได้อะไร ถ้าไม่บอกจะเกิดปัญหาซึ่งหลัก ๆ ที่พบจะเป็นปัญหาเรื่อง cross-sell คือพยายามขายผลิตภัณฑ์อื่นให้ แต่สำหรับ data subject กฎหมายคุ้มครองอยู่แล้วและเจ้าของข้อมูลสามารถใช้สิทธิ์ได้อยู่แล้ว หากไม่รู้ว่าบริษัทนำข้อมูลไปใช้งานตรงนี้ก็สามารถร้องเรียนได้ คิดว่าการถามคำถามนี้แปลว่าเริ่มเข้าใจแล้วว่าความคาดหมายของ data subject จะเป็นประเด็น เพราะฉะนั้นผู้ประกอบการจะต้องหาวิธีการว่าทำอย่างไรจึงจะทำให้ลูกค้าคาดหวังได้ ดังนั้นจึงขอตอบในฝั่งผู้ประกอบการว่าผู้ประกอบการจะต้องมีลูกเล่นทางการตลาด เช่น ถ้าลูกค้าอยากได้ของ ผู้ประกอบการก็จะบอกใน policy หรือใด ๆ ว่า ลูกค้าได้ให้ความยินยอมเพื่อที่จะให้ผู้ประกอบการติดต่อด้วย กล่าวคือจะแจ้งไว้ตั้งแต่ต้น เปรียบเสมือนการแลกเปลี่ยนกันเอาของแลกเพื่อให้ได้สิ่งนี้ นี่เป็น practice ปกติที่เกิดขึ้น

นายปริย

หากประยุกต์เรื่องนี้กับการขายการแนะนำ คือบอกว่าถ้าลูกค้าไปทำสัญญาขอให้ service เพื่อลงทุนผลิตภัณฑ์ ผู้ประกอบการควรจะโฟกัสที่การให้บริการผลิตภัณฑ์นั้นใช่หรือไม่ ถ้ามีการขยายผลไปที่ผลิตภัณฑ์อื่นที่ลูกค้าอาจจะไม่เคยคุยกันมาก่อน จะต้องถามลูกค้าก่อน ซึ่งปัจจุบันที่ทำกันอยู่คือ ถามไปตั้งแต่ผลิตภัณฑ์แรกที่คุยกันว่าลูกค้าจะยินยอมให้ผู้ประกอบการ approach ในการนำเสนอผลิตภัณฑ์อื่นหรือเปล่า ใช่หรือไม่

ผศ.ดร. ปิยะบุตร

ใช่

ดร. ไกรพิชิต

ต่อไปเป็นคำถามจากกลุ่มธุรกิจการสอบบัญชี กลุ่ม auditor มีคำถามที่สำคัญและน่าสนใจมากและยังสามารถนำมาประยุกต์ใช้กับธุรกิจอื่น ๆ ได้อีกด้วย คำถามคือ สำนักงานสอบบัญชีมีข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลที่ได้รับจากบริษัทลูกค้าที่เป็น data controller ไม่ได้รับจากเจ้าของข้อมูลหรือ data subject โดยตรง แม้ว่าสำนักงานสอบบัญชีจะถือว่าข้อมูลดังกล่าวได้มาและประมวลผลเพื่อปฏิบัติตามสัญญาที่มีต่อ data controller และมีการกำหนดมาตรฐานในการแจ้งบริษัทลูกค้าให้ทราบถึงความต้องปฏิบัติตามกฎหมาย แต่สำนักงานสอบบัญชีประเมินว่ายังมีความเสี่ยงต่อการไม่ปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กรณีบริษัทของลูกค้าซึ่งเป็น data controller ไม่ได้ดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบว่าจะต้องส่งข้อมูลให้กับสำนักงานสอบบัญชี คำถามคือสำนักงานสอบบัญชีในฐานะที่เป็น data processor คือประมวลผลข้อมูลตามคำสั่งของลูกค้าคือ data controller จะมีความเสี่ยงด้านกฎหมาย (Legal risk) หรือไม่ ถ้า data controller ทำงานไม่ครบถ้วนสมบูรณ์ไม่ถูกต้อง และ data processor ควรทำอย่าไรเพื่อปิดความเสี่ยงนี้

ผศ.ดร. ปิยะบุตร

มี 2 ประเด็นใหญ่ ประเด็นแรกคือสถานะของผู้สอบบัญชีเป็น processor กรณีนี้อาจจะต้องให้ดูเป็นรายกิจกรรม จากที่เข้าใจคือมีกิจกรรมที่สำนักงานสอบบัญชีจะต้อง exercise ความเป็น auditor ตามกฎหมายนั่นคือ

เป็น controller ไม่ใช่ processor เพราะว่าไม่ได้ทำตามคำสั่ง สำนักงานสอบบัญชีจะต้องใส่หมายเหตุซึ่งเรื่องนี้อาจารย์อาจจะเข้าใจเองอาจจะพูดผิดได้ หมายเหตุนั้นต้องเป็นการระบุว่าจะต้องเป็นเช่นนี้เพราะว่ามันเป็นวิชาชีพเป็นการ exercise บทบาทหน้าที่ของ controller กล่าวคือถ้าหมายเหตุนั้นเกี่ยวข้องกับข้อมูลส่วนบุคคลก็จะเป็นไปในลักษณะนั้น แต่หากเป็นงานที่ไม่ได้ exercise ความเป็นวิชาชีพ คือทำตามสัญญาแท้ๆ กรณีนี้จะเป็น processor

ประเด็นที่ 2 เรื่องความเสี่ยง คำถามนี้แสดงให้เห็นว่าคนถามเริ่มจะเข้าใจในเรื่องนี้ว่าการที่ได้รับข้อมูลมานั้น สำนักงานสอบบัญชีจะไม่ทราบเลยว่าต้นทางดูแลข้อมูลอย่างไรหรือได้มาถูกต้องหรือไม่ ซึ่งเป็นประเด็นที่น่าสนใจสำหรับเรื่องนี้ในปีนี้ วิธีการที่แนะนำโดยที่ปรึกษาทางกฎหมายว่าให้ทำเป็นหลัก คือเนื่องจากสำนักงานสอบบัญชีไม่สามารถทำแทนบริษัทลูกค้าได้ สมมติว่าต้นทางบริษัท A จ้างสำนักงานสอบบัญชีไปทำงานใด ๆ และมีการส่งข้อมูลส่วนบุคคลให้ประมวล วิธีการที่ทำคือในสัญญานี้จะต้องมีสิ่งที่ในทางกฎหมายเรียกว่า representation ว่าบริษัท A ได้ดำเนินตามกฎหมายนี้มาก่อนเรียบร้อยแล้ว สำนักงานสอบบัญชีไม่ต้องไปทำซ้ำอีก หลักการในทางปฏิบัติคือต้นทางต้องขอ consent ให้เสร็จเรียบร้อย ถ้าต้องมีการแจ้งก็ต้องแจ้งให้เรียบร้อย ไม่ใช่ภาระให้กับคนท่อนต่อ ๆ ไปต้องไปขอ consent หรือแจ้งอีก เพราะการที่ต้องไปขอ consent หรือแจ้งอีกจะเท่ากับการเริ่มนับ 1 ใหม่หมด มันเป็นไปไม่ได้ที่สำนักงานสอบบัญชีจะไปทำแบบนั้นด้วยตนเอง กรณีนี้จะเหมือนกับตัวอย่างก่อนหน้าที่อธิบายว่า โอกาสแรกที่โดนตัว data subject คือโอกาสที่จะแจ้งขอ consent หากเป็นโอกาสอื่นจะเป็นการนับ 1 ใหม่และทำได้ยาก โดยเฉพาะอย่างยิ่งการทำย้อนหลังจะทำให้รู้สึกว่ามันเป็นปัญหา ซึ่งอันที่จริงเรื่องนี้ในทางปฏิบัติไม่ให้ทำย้อนหลัง ต้องนับ 1 ใหม่

นายกำพล

ปกติผู้สอบบัญชีจะต้องสอบจากรายการที่บริษัท เช่น บริษัท A จ้างผู้สอบบริษัท B ลักษณะการสอบจะเป็นเรื่องการส่งข้อมูล transaction ทางบัญชีซึ่งแน่นอนว่าอาจมีข้อมูลที่เป็น privacy ของลูกค้าบริษัท เวลาส่งข้อมูลเกี่ยวกับ transaction ตัว data controller ยังคงเป็นบริษัทที่สั่งให้ทำ เพราะฉะนั้นการสืบต่อไปอีกทอดเช่นการสอบทุจริต คือมันเป็นไปไม่ได้ที่จะสอบตั้งแต่ต้น

ผศ.ดร. ปิยะบุตร

เข้าใจว่าคำถามน่าจะเป็นในลักษณะของการที่ลูกค้ามาทำธุรกรรมและมันยังไม่เกิดปัญหา แต่ว่าพออยู่ ๆ ไปลูกค้าเกิดมีปัญหา บริษัทจะกลับไปแจ้งขอ consent เพื่อทำการตรวจสอบจะเป็นไปไม่ได้ โจทย์น่าจะเป็นเช่นนี้ ดังนั้นวิธีการทำงานจะไม่ใช่การแจ้งตอนที่มีปัญหาแล้ว แต่จะต้องแจ้ง ณ โอกาสแรกที่ลูกค้าเข้ามา ว่าในกระบวนการทั้งหมดที่ลูกค้าจะต้องเจอประกอบด้วยอะไรบ้าง รวมถึงการตรวจสอบทุจริต การตรวจสอบบัญชีหรือการส่งต่อ regulator

ดร. ไกรพิชิต

คำถามต่อไปที่เกี่ยวกับข้อมูลส่วนบุคคลจาก auditor คือ ในบางกรณีที่สำนักงานสอบบัญชีจะเปิดเผยข้อมูลส่วนบุคคล เช่นการส่งมอบข้อมูลการลงทุนให้สำนักงานก.ล.ต. ข้อมูลของครอบครัวหุ้นส่วนหรือคนที่เกี่ยวโยงกัน ซึ่งโดยปกติไม่เคยต้องทำหนังสือขอความยินยอม จากพ.ร.บ. ฉบับนี้ ก็ไม่จำเป็นต้องขอความยินยอมใช่หรือไม่ เข้าใจว่าคำถามนี้จะเป็นลักษณะที่ว่า auditor ต้องแจ้งหรือเปิดเผยข้อมูลนั้นให้กับ regulator โดยข้อมูลนี้อาจจะไม่ใช่ข้อมูลของ data subject โดยตรง แต่เป็นข้อมูลของบุคคลอื่นที่เกี่ยวพันกับตัว data subject แบบนี้ต้องขอความยินยอมจากบุคคลอื่นที่เกี่ยวพันกับ data subject หรือไม่

ผศ.ดร. ปิยะบุตร

สำหรับคำถาม อยากให้ลงไปที่กิจกรรมจริง ๆ เพราะคำถามที่ถามมามีลักษณะเป็นการถามหลักการ ดังนั้นจะไม่ทราบว่ากิจกรรมนั้นเกิดขึ้นด้วยเหตุผลอะไร แต่จากที่คาดเดาน่าจะเป็นเหตุการณ์ที่ว่า regulator มีหนังสือเรียกให้สำนักงานสอบบัญชีส่งข้อมูลเนื่องจากบริษัทลูกค้ามีปัญหา เช่น ให้ส่งรายการมา กรณีเช่นนี้สำนักงานสอบบัญชีจะส่งได้ตามเหตุผลความจำเป็นตามกฎหมาย ส่วนวิธีการแจ้ง เนื่องจาก auditor ไม่ได้เป็นผู้ที่ปะทะกับ data subject โดยตรง ดังนั้นจะต้องกลับไปที่บริษัทลูกค้าที่จะต้องแจ้งตั้งแต่แรก สมมติว่าสำนักงานก.ล.ต. เป็น regulator ในกรณีนี้ ก็อาจจะมีข้อกำหนดบอกว่าบริษัทเหล่านี้จะต้องบอกหรือแจ้งเรื่องนี้ตั้งแต่แรกเพื่อให้ทราบว่าจะมีการส่งข้อมูล แต่ว่าไม่จำเป็นต้องเขียนละเอียดมาก อาจจะเขียนในลักษณะที่ว่า อาจจะมีเหตุการณ์ที่ต้องส่งข้อมูลไปให้ก.ล.ต. เพื่อเป็นการปฏิบัติตามกฎหมายการตรวจสอบทุจริตเพื่อบอกกว้างๆตั้งแต่แรกที่ยังไม่มีปัญหา

ดร. ไกรพิชิต

หากต้องการความชัดเจน จะต้องระบุกิจกรรมให้ชัดเจนมากกว่านี้เป็นรายๆไป เข้าใจว่าหลังจากนี้หากพบปัญหาในทางปฏิบัติ ทางสคส. และก.ล.ต. จะมีช่องทางให้ผู้ประกอบธุรกิจสามารถสอบถามหรือปรึกษาในรายละเอียดเพิ่มเติมได้ ต่อมาเป็นคำถามที่น่าสนใจโดยเฉพาะอย่างยิ่งกับกลุ่มธุรกิจใหม่ๆ นั่นก็คือธุรกิจ Fin Tech ตอนนี้กลุ่มผู้ประกอบธุรกิจสินทรัพย์ digital ยังไม่มีสมาคมกลางเหมือนกับธุรกิจอื่น ๆ เพราะฉะนั้นแนวทางการจัดทำนโยบายทางด้าน data privacy policy หรือการกำหนดแบบฟอร์มต่าง ๆ ที่ระบุว่าข้อมูลของธุรกิจนี้เป็นข้อมูลส่วนบุคคลอย่างเป็นความเห็นร่วมกันของทุกผู้ประกอบธุรกิจที่อุตสาหกรรมเดียวกัน ขอถามนายกำพลว่าสำนักงานก.ล.ต. มีคำแนะนำ หรือมีแนวทางในการให้ความช่วยเหลือกลุ่มผู้ประกอบธุรกิจที่ยังไม่มีสมาคมเป็นตัวกลางในการหาข้อตกลงร่วมกันในธุรกิจต่าง ๆ โดยเฉพาะอย่างยิ่งเรื่องการกำหนดมาตรฐานกลางของธุรกิจในการปฏิบัติตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลอย่างไร และมีความคาดหวังอย่างไร

นายกำพล

กลุ่มธุรกิจหลักๆจะมีทั้งหมด 14 กลุ่มตามที่กล่าวไว้ในตอนต้น และเมื่อเอ่ยถึงกลุ่มธุรกิจใหม่ เช่น Fin Tech Digital Assets หรือ ICO Portal จะเห็นได้จากผลการประเมินตนเองว่าเป็นกลุ่มที่ใช้เทคโนโลยีมาก มีการสร้างความปลอดภัย ทำ Privacy by design ตั้งแต่ต้นอยู่แล้ว เป็นกลุ่มที่มีความพร้อม แต่อย่างไรก็ตามเมื่อเป็นธุรกิจใหม่ การรวมตัวในลักษณะของสมาคมก็น่าจะมีสมาคมรองรับอยู่ ไม่ว่าจะเป็น สมาคมสินทรัพย์ digital ไทย สมาคม Fin Tech หรือสมาคม Blockchain แต่เนื่องด้วยสำนักงานก.ล.ต. เองไม่ได้เข้าไปเกี่ยวข้องโดยตรง จึงไม่มีข้อมูลชัดเจนว่า กลุ่มสมาคมเหล่านี้เป็นการรวมตัวกันในฐานะที่เป็นสมาคมผู้ประกอบการเหมือนสมาคมบริษัทหลักทรัพย์ สมาคมบริษัทหลักทรัพย์จัดการกองทุนรวมหรือไม่ หากเป็นไปได้ก็อาจจะยกระดับสมาคมเพื่อร่วมด้วยช่วยกัน แต่หากเป็นกลุ่มธุรกิจที่เพิ่งเกิดขึ้น คือเป็นกลุ่มของผู้ประกอบการเป็นการเฉพาะ ท่านสามารถเข้ามาที่ช่องทางของก.ล.ต. หรือสคส. โดยตรงเพราะเรียกได้ว่า 2 หน่วยงานนี้ทำงานประสานกันอย่างใกล้ชิดอยู่แล้วในลักษณะของการช่วยอำนวยความสะดวกเพื่อให้กลุ่มธุรกิจเหล่านี้สามารถปฏิบัติตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และจะสามารถผ่านเรื่องนี้ไปได้ด้วยดี เพราะไม่อยากเห็นใครที่จะต้องถูกลงโทษภายใต้กฎหมายใหม่ กฎหมายใหม่นี้น่าจะเป็นสิ่งที่ช่วยสร้างความเชื่อมั่นให้กับนักลงทุนไม่ว่าจะเป็นไทยหรือต่างชาติที่จะเข้ามาทำธุรกรรมหรือทำธุรกิจด้วย กฎหมายน่าจะเป็นส่วนช่วยในการใช้เป็นโอกาสในการขยายธุรกิจมากกว่าที่จะเป็นภาระของการกระทำ หากมีข้อสงสัยหรือปัญหาสามารถมาที่ก.ล.ต. ได้เพราะในส่วนของก.ล.ต. เองก็มีการตั้งคณะทำงานเพื่อช่วยเหลือกลุ่มธุรกิจอยู่แล้ว

ดร. ไกรพิชิต

ซึ่งท่านผู้ช่วยกำพลเป็นหัวหน้าคณะทำงานนี้ด้วยเช่นกัน คำถามข้อสุดท้ายนั้นไม่แน่ใจว่าเป็นคำถามหรือเป็นเสียงแสดงความคิดเห็นหรือเป็นเสียงบ่นจากผู้ประกอบธุรกิจ คำถามคือ ไม่มีหน่วยงานที่สามารถสอบถามและปรึกษาในข้อกฎหมายและการจัดเตรียมความพร้อมของบริษัทให้เป็นไปตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล จึงไม่สามารถสอบถามข้อมูลและรายละเอียดในเชิงลึกได้ อีกทั้งแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 2.0 ไม่ได้ครอบคลุมรายละเอียดในการดำเนินงานขององค์กร จะเห็นว่าผู้ที่ถามคำถามนี้ ได้พยายามเตรียมการด้วยตัวเองแล้ว แต่มีคำถามในเชิงลึกหรือมีคำถามในเชิงปฏิบัติเพิ่มมากขึ้น จึงคาดหวังความช่วยเหลือหรือความชัดเจนจากหน่วยงานภาครัฐ ขอถามทั้ง 2 ท่านทั้งนายกำพลและอ.ปิยะบุตรในฐานะที่ปรึกษาของสคส. ว่าทางภาครัฐโดยเฉพาะอย่างยิ่งเป็น regulator ของ PDPA หรือ Federal regulator อย่างก.ล.ต. จะเตรียมการช่วยเหลือภาคธุรกิจในประเด็นนี้อย่างไร ก่อนหน้านี้มีการพูดถึงประเด็นนี้ในเชิงหลักการแล้ว จึงอยากทราบแนวทางที่ชัดเจนหรือการจัดตั้งหน่วยงานหรือคณะขึ้นมาเพื่อสนับสนุนช่วยเหลืออย่างไร ทั้งจากทางกระทรวง DES เองหรือจากก.ล.ต. เอง

ผศ.ดร. ปิยะบุตร

ณ ปัจจุบันตอนนี้สำนักงานสคส. ซึ่งดำเนินการโดยสำนักงานปลัดของกระทรวง DES จะมีส่วนงานที่ถูกมอบหมายมาให้ดำเนินการเป็นหลักอยู่แล้วส่วนหนึ่ง ทุกวันนี้ทางอาจารย์จะได้รับคำถามและพยายามตอบคำถามต่าง ๆ ที่เข้ามา คือพยายามอำนวยความสะดวกเท่าที่ทรัพยากรจะเอื้ออำนวย แต่สำหรับคำถามในเชิงลึกอาจจะขอให้บริษัทใช้เวลาสักนิด ทุกวันนี้สคส. เองจะมีที่ปรึกษาคอยช่วยตอบคำถามอยู่ตลอด ดังนั้นหากมีประเด็นสามารถถามมาได้ กลุ่มที่ปรึกษาพยายามช่วยตอบให้อยู่แล้ว กรณีที่ถามมาอาจจะเป็นไปได้ว่าเมื่อถามคำถามเชิงลึกที่ลงไปในบริบทของบริษัทนั้นอย่างเฉพาะเจาะจงมาก ๆ เวลาถามอาจจะถามลงลึกได้ไม่มาก ดังนั้นทางคณะจึงไม่รู้จะตอบอย่างไร ตัวอย่างเช่นเมื่อครู่มีหลาย ๆ คำถามที่พยายามจะชี้ให้เห็นว่า หากมีรายละเอียดหรือบริบทของเรื่องที่ชัดเจนก็จะตอบได้ซึ่งส่วนใหญ่ปัญหาที่พบจะเป็นแบบนี้

ส่วนแนวปฏิบัติ 2.0 คือไม่มีทางที่จะครอบคลุมทุกเรื่องได้แน่นอนซึ่งทางคณะเข้าใจดี จึงขอถือโอกาสนี้ promote ว่า ในอนาคตจะมี version 3.0 ซึ่งจะลงรายละเอียดของแต่ละองค์กรมากขึ้น จะดูในเรื่อง HR IT Security Procurement Marketing ให้ละเอียดลงไปใน business function หลัก ๆ จะเป็นเช่นนี้

นายกำพล

สิ่งนี้แสดงให้เห็นถึงความมุ่งมั่นของสคส. เพราะอ.ปิยะบุตรก็เป็นหนึ่งในที่ปรึกษาของสคส. และมี commitment อยู่หลายภาคส่วน ดังนั้นแน่นอนว่ามีการเตรียมการที่จะช่วยเหลืออยู่แล้ว ในส่วนของก.ล.ต. เอง จากที่ได้ดูคำถามจาก Slido ปรากฏว่าคำถามที่เข้ามาเป็นคำถามในเชิงลึกเกินกว่าที่จะให้สคส. ตอบโดยลำพัง เพราะเป็นคำถามเฉพาะในกลุ่มของตลาดทุน ไม่ใช่เพียงตลาดทุนเท่านั้น ยังมีผู้ประกอบธุรกิจแต่ละด้านซึ่งเป็นการยากพอสมควร จึงอยากเรียนให้ผู้ประกอบการสบายใจว่าก.ล.ต. เองเป็นหน่วยงานหนึ่งที่ร่วมมือใกล้ชิดกับสคส. หลายประเด็นจะเป็นเรื่องความรู้ความเข้าใจในการทำธุรกรรมระหว่างกัน ความจำเป็นในการใช้ข้อมูลส่วนบุคคลต่าง ๆ ซึ่งเป็นสิ่งที่ก.ล.ต. ต้องทำความเข้าใจ อย่างไรก็ตามในบริบทที่เป็นความต้องการในส่วนของกฎหมาย PDPA และด้วยเจตนารมณ์หลายๆเรื่องจะต้องประสานงานกันอย่างใกล้ชิด สำนักงานก.ล.ต. เองมีการตั้งคณะทำงานเป็นการเฉพาะ เพื่อดูแลกลุ่มผู้ประกอบธุรกิจทั้ง 14 กลุ่ม ซึ่งนอกจากจะมีตัวท่านผู้ช่วยเลขาเอง ดร. ไกรพิชิต ก็จะมีผู้อำนวยการฝ่ายของทุก ๆ business unit เข้าร่วมเป็นคณะทำงาน เพื่อดูแลภาคอุตสาหกรรม และการประสานงานกับสคส. ซึ่งน่าจะเป็นอีกช่องทางที่ทำให้ผู้ประกอบการมั่นใจว่าทุก ๆ ปัญหาหรือข้อสงสัยจะได้รับการช่วยเหลือ นอกจากนี้ในเรื่อง Security by design ที่มีการทำมาตั้งแต่ต้น สำนักงานก.ล.ต. เองมีเกณฑ์ในเรื่อง information security ที่เข้มงวด สิ่งนี้น่าจะช่วยสร้างความมั่นใจให้กับผู้ที่มาใช้บริการ ว่าข้อมูลต่าง ๆ จะได้รับการดูแลเป็นอย่างดี กรณีที่กฎหมาย PDPA มีความต้องการเพิ่มขึ้น เช่น ต้องการให้ดูแลข้อมูลส่วนบุคคลเป็นพิเศษมากขึ้น อาจจะต้องมีเรื่องการทำ encryption การแปลงรหัส anonymize ต่าง ๆ เหล่านี้ในอนาคตอาจจะมีการหารือกับทางสคส. ผ่านทางกรรมการว่าจะมีระเบียบ กฎหมายลูกอะไรที่เกี่ยวข้องหรือไม่ อยากให้มั่นใจว่าทางก.ล.ต. จะดูแลด้วยใจ นอกจากนี้การที่ท่านเลขาธิการก.ล.ต. เป็นคณะกรรมการทางด้านการเงิน นอกเหนือจากตลาดทุนรวมไปถึงธนาคาร ประกันภัย คิดว่าท่านเลขาธิการจะช่วยดูแลและช่วยอำนวยความสะดวกให้ผ่านกฎหมายไปด้วยดีเช่นกัน

ดร. ไกรพิชิต

ในการประเมินความพร้อมของภาคธุรกิจในตลาดทุนที่ผ่านมา จะเห็นว่าหลายๆภาคส่วนและภาคอุตสาหกรรมมีความตื่นตัวในเรื่องนี้และมีความพยายามที่จะดำเนินการเพื่อให้มีความพร้อมในการ comply ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งถือว่าเป็นสัญญาณที่ดี แสดงให้เห็นว่าผู้ประกอบธุรกิจได้เริ่มดำเนินการแล้ว เห็น awareness เห็นความสำคัญต่อการปฏิบัติตามกฎหมายและต่อภาคธุรกิจด้วย อยากให้ผู้ประกอบธุรกิจดำเนินการเรื่องนี้ต่อไปจนสุดทาง ซึ่งในระหว่างนี้เองทาง ก.ล.ต. และสคส. ก็จะไปพร้อมกัน โดยช่วยเหลือให้ทุกบริษัททำได้อย่างครบถ้วนถูกต้อง อย่างไรก็ตามเชื่อว่าอาจจะยังมีประเด็นคำถามที่ยังติดใจผู้ประกอบธุรกิจอยู่

ตอนนี้ทางสำนักงาน ก.ล.ต. กำลังเตรียมพร้อมเรื่องการจัดทำ website เพื่อรวบรวมคำถามและคำตอบเป็น FAQ ซึ่งจะเผยแพร่บน website ของสำนักงาน ก.ล.ต. เองเพื่อเป็น knowledge management ที่รวบรวมคำถาม คำตอบที่สามารถนำไปใช้ต่อยอด โดยจะมีการเปิด website ได้เร็วๆนี้ ทางสำนักงานเองจะพยายามเร่งดำเนินการอย่างดีที่สุด