ตอบคำถามสัมมนา PDPA

ลำดับ	คำถาม	คำตอบ
การเตรียมความพร้อม PDPA		
1	GDPR กับ PDPA ค่าปรับต่างกัน ถ้าคนยุโรปอยู่ในเมืองไทยจะใช้ค่าปรับของกม. ไหน	หากเป็นเรื่องเดียวกัน ความเห็นคือ ไม่ควรจะมีการลงโทษสำหรับการกระทำความผิดหลายครั้งในเรื่องเดียวกัน (Double Jurisdiction) กฎหมายจึงกำหนดให้หน่วยงานกำกับ ปรึกษาหารือกัน หากเป็นการกระทำที่เข้าข่ายทั้งสองบทกฎหมาย เราก็จะทำการรายงานหน่วยเกี่ยวข้องของทุกประเทศที่เกี่ยวข้อง เช่นทั้งประเทศที่บุคคลดังกล่าวถือสัญชาติ และประเทศไทย แต่การลงโทษจะเป็นของประเทศใด เห็นว่าหน่วยงานกำกับ ควรจะต้องปรึกษาหารือกัน
		<u>กรณีที่ PDPA มีผลบังคับใช้</u> ถ้ากิจกรรมการประมวลผลข้อมูลส่วนบุคคลของทางบริษัทในประเทศไทย ไม่อยู่ในขอบเขตตามกฎหมายของ GDPR เช่น บริษัทไม่มีสำนักงานหรือเสนอขายสินค้าและ/หรือบริการโดยตรงแก่ลูกค้าในขอบเขต เป็นต้น อาจใช้ค่าปรับตาม PDPA อย่างเดียว **<u>ตัวอย่าง</u>** บริษัทที่ประกอบกิจการเครือร้านอาหารในประเทศไทย ซึ่งไม่มีสาขาของร้านที่ยุโรป และไม่ได้มีการกิจกรรมนำเสนอขายบริการร้านอาหารของบริษัทโดยตรงในยุโรป เช่นออกบูทประชาสัมพันธ์ โรดโชว์ เป็นต้น ข้อมูลรั่วไหลกรณีที่ลูกค้ามาท่องเที่ยวในประเทศไทยและใช้บริการของร้านอาหารในเครือทางบริษัท จะอยู่ภายใต้ PDPA เท่านั้น (กรณี PDPA มีผลบังคับใช้)
2	สวัสดีค่ะ มีคำถามขอเรียนทางท่านวิทยากร เรื่อง การเขียนรายงาน 56-1 และ 56-1 One Report ซึ่งจะเชื่อมโยงระหว่างหัวข้อ ธุรกิจกับสิทธิมนุษยชน กับ หัวข้อการแสดงข้อมูลการจัดการด้านความยั่งยืน HR1-3 มีข้อแนะนำว่าให้รวมอยู่ด้วยกัน โดยใช้เรื่อง human rights เป็นหัวข้อใหญ่ไหมคะ // หรือให้แยกหัวข้อกันไปเลยดีกว่าคะ?	ถ้าลักษณะของกิจกรรมเหมือนกันก็อยู่รวมกันได้ แต่หากมีข้อแตกต่างในสาระสำคัญก็สามารถแยกเพื่อความชัดเจนได้

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

3	มีแนะนำ บริษัทฯหรือองค์กรที่ให้บริการ Application ด้าน PDPA ไหมครับ เช่น System ต่างๆ ROPA, Data Flow, Rights & Access to Data, Use & Disclosure of Data, Rejection of request, Report a violation หรือกรณีอื่นๆ ที่เกี่ยวข้อง	- กรณี Data Flow แนะนำเป็น Visio - กรณี Cookies แนะนำเป็น One Trust หรือ Cookiebot - กรณี Rights & Access to Data แนะนำเป็น Saviynt, Onelogin และCyberArk ซึ่งเป็นระบบ Identity and Access Management - ส่วนกรณี Consent Management บริษัทฯ อาจจะไม่สามารถแนะนำระบบได้ เนื่องจากระบบของบริษัทฯ มีลักษณะเฉพาะตัวจึงได้มีการพัฒนาระบบขึ้นเอง
		กลุ่มธุรกิจการเงินเกียรตินาคินภัทรไม่ได้ใช้ Application อะไรเป็นการเฉพาะ โดยในกระบวนการทำงานทั้งหมดฝ่าย IT, PDPA Team, Operation ร่วมกันออกแบบ work flow และ system ที่เขียนขึ้นมาเองเพื่อใช้ในกลุ่มธุรกิจเพื่อให้เป็นไปตาม requirement ของกฎหมาย และมีฝ่าย Internal Audit และ Risk Management เข้ามาร่วมประเมินทุกกระบวนการในการทำงานของ PDPA Team ตั้งแต่เริ่มจนถึงเสร็จสิ้นกระบวนการ รวมถึงมีการทำประเมินความเสี่ยงอย่างต่อเนื่องด้วย
4	ในกรณีที่บริษัทถ่ายรูปหน้าพนักงาน เพื่อใช้ในการ Scan เข้าออกงาน โดยเก็บเพียงรูปถ่าย แต่ไม่ได้เก็บความลึกตื้นหนาบางหรือโครงหน้าอันเป็นข้อมูลชีวะ ในส่วนนี้ถือว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือไม่ครับ และต้องขอความยินยอม หรือทำเป็น Privacy Notice ก็เพียงพอแล้วครับ	ลำพังเพียงรูปถ่ายไม่ได้มีการนำไปวิเคราะห์เพื่อหาโครงสร้างของใบหน้าหรือข้อมูล Biometric เป็นข้อมูลส่วนบุคคลทั่วไป หากสามารถอ้างความจำเป็นวัตถุประสงค์ตามมาตรา 24 ได้ ไม่จำต้องขอความยินยอม
5	บริษัทต้องทำอย่างไรในทางปฏิบัติ? เพื่อรองรับ พรบ.คุ้มครองข้อมูลส่วนบุคคล	ท่านสามารถศึกษาแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ของคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย (TDPG 3.0)
6	ลูกค้าเก่าหรือ prospect ที่เคยเก็บมาก่อนวันที่ 1 มิ.ย. 65 ต้องขอ consent ก่อน	ต้องพิจารณากิจกรรมก่อนว่าเป็นกิจกรรมอะไร ถ้าเกิดไม่ใช่กิจกรรมที่ต้องขอ consent ไม่ต้องมีการขอ consent แต่ถ้าเป็นฐาน consent ก็ต้องมีการขอใหม่ ต่อให้เคยขอ consent ไปแล้วก็ควรที่จะมีการขอใหม่เมื่อกฎหมายใช้บังคับเพราะบางทีการขอ consent เดิมอาจไม่ได้มาตรฐานตาม PDPA
7	อยากทราบว่าสำนักงาน จะมีการออก guideline ให้กับกลุ่มธุรกิจมั้ยคะ เหมือนกับของ คปภ และ ธปท.	สำนักงานให้การสนับสนุนแนวปฏิบัติของสมาคมต่างๆ ภายใต้การกำกับดูแลของสำนักงาน และสมาคมจะมีการทำ public hearing ซึ่งสามารถนำมาใช้เป็นแนวทางในการดำเนินการได้

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

8	มีตัวอย่าง โครงสร้างของคณะทำงาน PDPA (รวมถึง DPO Structure) ไหมคะ	โครงสร้างของ PDPA Team ของกลุ่มธุรกิจการเงินเกียรตินาคินภัทร อยู่ภายใต้สายงาน Legal and Compliance จะประกอบด้วย DPO ที่เป็นนักกฎหมาย และบุคลากรที่มาจากฝ่าย Compliance ที่มีประสบการณ์ด้าน IT, กระบวนการทำงาน, และ ทีมดูแลกฎเกณฑ์ที่เกี่ยวข้องกับ ปปง. หรือกระบวนการรับลูกค้า โดย DPO จะได้รับการแต่งตั้งจาก Board ของทุกบริษัทในกลุ่มธุรกิจฯ และมีหน้าที่รายงานตรงไปยัง Board หรือคณะกรรมการที่ Board มอบหมาย นอกจากนี้ DPO ยังเป็นคณะทำงานที่ดูแลด้าน Data Governance เพื่อดูแลให้การประมวลผลข้อมูลต่างๆ ของกลุ่มธุรกิจฯ เป็นไปตามที่กฎหมายและระเบียบต่างๆ กำหนด ส่วนการประสานงานกับฝ่ายงานอื่นๆ จำต้องมีการแต่งตั้งผู้ประสานเป็น PDPA champion เพื่อเป็นผู้คอยประสานงานและดูแลให้ฝ่ายงานของตนสามารถปฏิบัติงานได้ตามที่กฎหมายหรือระเบียบต่างๆ กำหนด **โครงสร้างคณะทำงาน PDPA ของบริษัทบริษัท เอก-ชัย ดีสทริบิวชั่น ซิสเทม จำกัด (โลตัส) โดยย่อมีดังนี้** 1. Compliance, Risk and Sustainability Committee (CRSC) : ซึ่งเป็นคณะกรรมการที่คอยกำกับดูแลด้านความเสี่ยงและการปฏิบัติตาม กฎเกณฑ์และคอยกำหนดทิศทางของบริษัทฯ ให้เป็นไปตามหลักธรรมาภิบาล ซึ่งคณะกรรมการชุดดังกล่าวประกอบไปด้วยผู้บริหารระดับสูงจากทุกสายงานและมี CEO เป็นประธาน 2. Privacy Committee: ซึ่งเป็นคณะกรรมการย่อยที่ได้รับการแต่งตั้งจากคณะกรรมการ CRSC มีหน้าที่กำกับดูแลด้านข้อมูลส่วนบุคคลโดยเฉพาะ โดยคณะกรรมการนั้นเป็นผู้บริหารระดับสูงที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคลโดยตรง เช่น Marketing HR IT Legal และ Security 3. DPO & Data Manager: ในส่วนของ Data Manager นั้น มีการแต่งตั้งมาจากสองหน่วยงานที่สำคัญๆ ที่มีการใช้ข้อมูลส่วนบุคคลจำนวนมาก นั่นคือหน่วยงาน Customer และ HR ทั้งนี้เพื่อเข้ามาดูแลเรื่องข้อมูลส่วนบุคคลที่เกี่ยวข้องโดยเฉพาะ อีกทั้งสนับสนุนการดำเนินการตาม Privacy Compliance Program (PCP) ของบริษัทฯ 4. Project Manager: เนื่องจากการดำเนินการตาม PCP ของบริษัทฯ นั้นจะประกอบไปด้วย activities จำนวนมาก จึงมีความจำเป็นที่จะต้องมี Project Manager เพื่อคอยช่วยติดตามการทำงานและความคืบหน้าในแต่ละ activities ให้เป็นไปตามกรอบการทำงานที่บริษัทฯ กำหนด 5. Data Protection Champion: ตัวแทนในการประสานงานด้าน Privacy ของแผนกที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มีจำนวนประมาณ 30 ท่าน **DPO** บริษัทฯ มี DPO 1 คน ซึ่งอยู่ภายใต้ฝ่ายกฎหมาย อย่างไรก็ตาม DPO จำเป็นที่จะต้องได้รับการสนับสนุนจากทุกภาคส่วนที่เกี่ยวข้องในองค์กรเพื่อประโยชน์สูงสุด

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

9	กรณีนายจ้างจัดทำประกันกลุ่มอันเป็นสวัสดิการให้แก่พนักงานนอกเหนือจากที่กฎหมายแรงงานกำหนด โดยบริษัทประกันจะส่งแบบฟอร์มมาให้นายจ้างเพื่อให้นายจ้างนำไปให้พนักงานกรอก โดยแบบฟอร์มจะเก็บข้อมูลส่วนตัวพนักงาน บิดา มารดาคู่สมรส ผู้รับประโยชน์ แต่ไม่ได้เก็บข้อมูลสุขภาพใดๆเลย เมื่อพนักงานกรอกข้อมูลเสร็จ นายจ้างจะเก็บรวบรวมเพียงรายชื่อพนักงานใส่ไฟล์ Excel ไปให้บริษัทประกัน ไม่ได้ส่งข้อมูลส่วนตัวพนักงาน บิดา มารดาคู่สมรส ผู้รับประโยชน์ไปด้วย และตัวแบบฟอร์มนายจ้างจะเก็บใส่แฟ้มไว้ที่ออฟฟิศไม่ได้ส่งให้บริษัทประกัน กรณีนี้ถือว่า นายจ้าง หรือ บริษัทประกัน เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีหน้าที่ในการขอความยินยอม หรือ แจ้งการประมวลผลข้อมูลส่วนบุคคลครับ หากบริษัทประกันเป็นผู้ควบคุมข้อมูลส่วนบุคคล นายจ้าง มีหน้าที่อย่างไร จะสามารถจัดเก็บตัวแบบฟอร์มไว้ได้หรือไม่	กิจกรรมนี้บริษัทประกันควรดำเนินการกับพนักงานเอง นายจ้างไม่ควรเก็บข้อมูลของพนักงาน(เก็บแบบฟอร์ม) แต่หากนายจ้างจะเก็บข้อมูลด้วยจะต้องทำ processing agreement โดยบ.ประกันจะเป็นผู้ควบคุม และนายจ้างจะเป็นผู้ประมวลผล
10	ในกรณีที่บริษัทจำเป็นต้องอัดเสียงพนักงานทางโทรศัพท์ที่ทำงานที่เป็น access persons เพื่อให้เป็นไปตามประกาศ ก.ล.ต. บริษัทจำเป็นต้อง แจ้งให้ผู้โทรเข้ามาว่าบริษัทมีการอัดเสียงหรือไม่	หากเรื่องที่อัดเพื่อการปฏิบัติงานให้เป็นไปตามประกาศของสำนักงาน ทางบริษัทต้องจัดทำ privacy policy โดยใช้ฐานกฎหมาย legal obligation และแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบในขั้นตอนก่อนประมวลผลข้อมูล

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

11	กรณีข้อมูลที่ถือว่าเป็นฐานสัญญาเราต้องแสดงให้ลูกค้าทราบได้อย่างไรว่าข้อมูลอะไรบ้างเป็นฐานสัญญา	ต้องพิจารณาตามกิจกรรมที่ทำว่าเป็นสัญญาหรือไม่ ไม่สามารถพิจารณาจากตัวข้อมูลได้
12	กลุ่มธุรกิจสถานพยาบาล ต้องดำเนินการอย่างไรบ้างในทางปฏิบัติ เพื่อให้รองรับกับ พรบ. นี้	ธุรกิจสถานพยาบาลเป็นธุรกิจที่มักมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวจึงต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม อาจเริ่มจากการจัดหมวดหมู่ประเภทข้อมูล จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูล และนโยบายคุ้มครองข้อมูลส่วนบุคคล
13	กรณีที่บางธนาคารได้ใช้วิธีการยืนยันตัวตนตามประกาศใหม่ของ ปปง โดยให้ส่งสำเนาบัตรประชาชนไปยังธนาคาร แต่ให้มีการขีดข้อมูลศาสนา หรือข้อมูลอ่อนไหวออก กรณีมีการทำแบบนี้ถือว่าถูกต้อง หรือมีความจำเป็นหรือไม่ครับ ที่เข้าใจว่า มาตรา 4 น่าจะได้รับการยกเว้นไม่ต้องปฏิบัติตามครับ	ถือว่าถูกต้องและควรทำในการขีดฆ่าข้อมูลที่ไม่มีความจำเป็นออกโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเพื่อไม่ให้มีการจัดเก็บตั้งแต่แรก ทั้งนี้การดำเนินการของธนาคารโดยหลักแล้วไม่ได้เข้าข้อยกเว้นตามมาตรา 4
14	1. แบบฟอร์มขอความยินยอมเก็บข้อมูลฯ ของลูกค้าที่มาขอสินเชื่อ หากมีเพียงช่อง ยินยอม เพียงอย่างเดียวสามารถทำได้หรือไม่ 2. แบบฟอร์มสามารถระบุประโยค " ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่ให้ความยินยอม บริษัทฯ ขอสงวนสิทธิ์ในการพิจารณาสินเชื่อ หรือวงเงินสินเชื่อ" ได้หรือไม่	1) ฐานขอความยินยอม ต้องมีทั้งปุ่ม ให้ความยินยอม และ ไม่ให้ความยินยอม โดยแยกกันชัดเจน และเจ้าของข้อมูลสามารถถอนความยินยอมได้ และการให้ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ 2) ไม่ได้

*** *คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม*

15	ขอทราบแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล บริษัทต้องจัดทำนโยบายแยกสำหรับบุคคลทั่วไป ลูกค้า พนักงาน ผู้ถือหุ้นและกรรมการ หรือไม่ หรือสามารถทำเป็นฉบับเดียวกัน	ขึ้นอยู่กับกิจกรรมของบริษัท ไม่ได้มีบทตายตัวค่ะ
16	ในการประกอบธุรกิจประกันภัยในประเทศไทย มีโอกาสจะถูกกำหนดให้เป็นการใช้ข้อมูลส่วนบุคคลในฐานประโยชน์สาธารณะที่สำคัญ (substantial public interest) ตามแบบของกฎหมายของประเทศอังกฤษบ้างหรือไม่	ขึ้นอยู่กับกิจกรรมการประมวลผล อย่างไรก็ตามส่งเสริมให้มีการทำแนวปฏิบัติสำหรับภาคกลุ่มธุรกิจประกันภัยเพื่อเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องตาม PDPA และเหมาะสมกับการดำเนินกิจกรรมของตน
17	1. อยากขอคำแนะนำของ Scope of work ที่ DPO ควรจะทำภายในองค์กรค่ะ 2. ลูกค้าเก่าที่เคยส่งข้อมูล Marketing ให้ ในอนาคตยังคงส่งต่อได้หรือไม่ หากไม่มีการขอความยินยอมใหม่ 3. Compliance ควรจะลงไปกำกับอย่างไรบ้าง เมื่อPDPAมีผลบังคับใช้	1. โดยหลักแล้วเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่เป็นไปตามมาตรา 42 กล่าวคือให้คำแนะนำและตรวจสอบการดำเนินงานภายในให้เป็นไปตามพรบ.คุ้มครองข้อมูลส่วนบุคคลฯ 2. ควรขอความยินยอมใหม่เพื่อให้ดำเนินการได้อย่างถูกต้องสอดคล้องตาม PDPA 3.ตรวจสอบเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรให้เป็นไปตามมาตรฐาน PDPA
18	ลูกค้าเก่าที่บริษัทเก็บสำเนาบัตรปชช.ไว้ ซึ่งมีข้อมูลศาสนาที่เป็นข้อมูลอ่อนไหว ควรต้องดำเนินการอย่างไรกับเอกสารดังกล่าว และต้องขอความยินยอมย้อนหลังหรือไม่คะ	สามารถเก็บต่อไปได้ตามวัตถุประสงค์เดิม โดยต้องกำหนดวิธีการยกเลิกความยินยอมและประชาสัมพันธ์สัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลทราบ ตามช่องทางการติดต่อโดยปกติระหว่างบริษัทและลูกค้า
19	การส่งข้อมูลของ ลค ไปให้ fb เพื่อให้ fb ส่งโฆษณาไปที่ fb account ของลค นั้น นอกเหนือจากต้องได้รับ data cross boarder consent นั้น ยังต้องได้รับ consent อื่นอีกหรือไม่ ถ้าต้องได้รับ consent ประเภทอื่น ควรจะเป็น marketing consent ใช่หรือไม่	ในการขอความยินยอมให้มีเนื้อหาเป็นไปตาม PDPA เช่น ข้อมูลเกี่ยวกับผู้ควบคุมฯ วัตถุประสงค์ในการประมวลผล วิธีการประมวลผล การโอนข้อมูลไปต่างประเทศ การเปิดเผยข้อมูลต่อบุคคลอื่น เป็นต้น

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

20	Singapore จะถูกประกาศเป็นประเทศใน whitelist ของ pdpa หรือไม่	ต้องรอคณะกรรมการประกาศกำหนด
21	ในกรณีมีให้ตอบก่อนใช้บริการว่า ยินยอมให้ใช้ข้อมูลส่วนบุคคลทางการตลาดหรือไม่ พอตอบไม่ระบบไม่ไปหน้าต่อไป ถือว่าผิดไหม บังคับลูกค้าไหม ทำได้หรือไม่ ใครเป็นคนควบคุมดูแลในส่วนนี้	หลักของความยินยอมต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญ จะนำมาใช้เป็นเงื่อนไขในการให้ความยินยอมที่ไม่มีความจำเป็นหรือเกี่ยวข้องกับการเข้าทำสัญญาหรือใช้บริการไม่ได้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดทำการขอความยินยอมให้เป็นไปตาม PDPA
22	จะมีการประกาศกฎหมายลูกเมื่อไหร่ และจะมีเวลาเพียงพอให้ภาคธุรกิจดำเนินการหรือไม่ (grace period)	การประกาศกฎหมายลำดับรองฯ ต้องรอคณะกรรมการประกาศกำหนด สำหรับตอนนี้ภาคธุรกิจสามารถเริ่มดำเนินการโดยพิจารณาตาม PDPA เป็นหลักไปก่อนได้ ประกอบกับการอิงตามแนวเอกสารผลการรับฟังความเห็นเกี่ยวกับ (ร่าง) กฎหมายลำดับรองฯ
23	ขอทราบวิธีปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลบริษัทมีอยู่ก่อนกฎหมายบังคับใช้ ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล วิธีการอย่างไร หากไม่ได้แจ้งจะมีผลอย่างไร	ต้องพิจารณากิจกรรมก่อนว่าเป็นกิจกรรมอะไร ถ้าเกิดไม่ใช่กิจกรรมที่ต้องขอ consent ไม่ต้องมีการขอ consent แต่ถ้าเป็นฐาน consent ก็ต้องมีการขอใหม่ ต่อให้เคยขอ consent ไปแล้วก็ควรที่จะมีการขอใหม่เมื่อกฎหมายใช้บังคับเพราะบางทีการขอ consent เดิมอาจไม่ได้มาตรฐานตาม PDPA
24	ขอทราบแนวทางในการจัดการลูกค้าเดิมที่มีอยู่ ว่าต้องขอconsentในการแชร์ข้อมูลในพันธมิตรธุรกิจหรือไม่ ถ้าต้องขอจะเป็นอุปสรรคในการดำเนินการอย่างมาก	ต้องพิจารณากิจกรรมก่อนว่าเป็นกิจกรรมอะไร ถ้าเกิดไม่ใช่กิจกรรมที่ต้องขอ consent ไม่ต้องมีการขอ consent แต่ถ้าเป็นฐาน consent ก็ต้องมีการขอใหม่ ต่อให้เคยขอ consent ไปแล้วก็ควรที่จะมีการขอใหม่เมื่อกฎหมายใช้บังคับเพราะบางทีการขอ consent เดิมอาจไม่ได้มาตรฐานตาม PDPA
25	ในการจัดทำสัญญามีความจำเป็นหรือไม่ที่จะต้องระบุเงื่อนไขการปฏิบัติตาม พรบ.คุ้มครองข้อมูลส่วนบุคคลลงไปในสัญญาทุกฉบับ	ไม่จำเป็น แต่ต้องมีการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบตามมาตรา 23
26	สำนักงานจะจัดทำ guideline เพื่อช่วยในการจำแนกประเภทกิจกรรมทางการตลาดของกลุ่มธุรกิจ บล บลจ. ให้หรือไม่ว่า กิจกรรมประเภทใดควรใช้ฐานสัญญาหรือฐาน legitimate interest เช่นเดียวกับที่ ธปท. ทำให้กลุ่มธนาคาร	สำนักงานให้การสนับสนุนแนวปฏิบัติ ของสมาคมต่างๆ ภายใต้การกำกับดูแลของสำนักงาน และสมาคมจะมีการทำ public hearing ซึ่งสามารถนำมาใช้เป็นแนวทางในการดำเนินการ

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

27	กรณีที่เป็นการทำการตลาดกับผู้เยาว์ (อายุต่ำกว่า 20 ปี) ต้องขอความยินยอมจากผู้แทนโดยชอบธรรม หรือผู้ใช้อำนาจปกครองตามกฎหมายหรือไม่อย่างไรคะ	การขอความยินยอมผู้เยาว์ต้องใช้ภาษาที่เข้าใจได้ง่าย คำนึงถึงความสามารถในการเข้าใจวัตถุประสงค์และรายละเอียดของการประมวลผลของผู้เยาว์ หากไม่ใช่กรณีที่ผู้เยาว์สามารถให้ความยินยอมโดยลำพังได้ตามที่กำหนดไว้ในประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองด้วย ส่วนกรณีที่ผู้เยาว์อายุไม่เกิน 10 ปี ต้องขอความยินยอมจากผู้ใช้อำนาจปกครอง
28	Record of Processing Activities ตามมาตรา 39 จำเป็นต้องทำเป็นบันทึกรวมกันไว้ในเอกสารเดียวหรือไม่หรือสามารถแยกส่วนกันได้ครับ	ควรรวมไว้ในเอกสารเดียวเพื่อให้ง่ายต่อการบันทึกและการตรวจสอบ
29	การ Store ข้อมูลใน Cloud ต่างประเทศ เป็น Transfer of data หรือ Transit of data คะ ในกรณีนี้ส่วนใหญ่ Cloud service ในต่างประเทศ ก็สามารถ Access ข้อมูลได้ ขอบคุณมากค่ะ	เป็น Transfer
30	การที่ลูกค้าเคยให้ความยินยอมในการเสนอขายผลิตภัณฑ์ แต่ต่อมาลูกค้าแจ้งว่าห้ามโทรขาย ถือว่ากรณีดังกล่าวเป็นกรณีที่ลูกค้าขอเพิกถอนการให้ความยินยอมหรือไม่ แล้วต้องดำเนินการในเรื่องดังกล่าวอย่างไร	ถือได้ว่าเป็นการเพิกถอนความยินยอมแล้ว เพื่อความชัดเจนควรมีช่องทางเพิกถอนความยินยอมและประชาสัมพันธ์ให้กับเจ้าของข้อมูลส่วนบุคคลทราบ เมื่อเจ้าของข้อมูลส่วนบุคคลเพิกถอนต้องยุติการประมวลผลข้อมูลส่วนบุคคลนั้น
31	การจัดเก็บกิจกรรมประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องเก็บในลักษณะใด ต้องแยกตามรายลูกค้าและบันทึกทุกกิจกรรมที่เกิดขึ้นในทุกวันเลยหรือไม่ หรือต้องมี excel file แยกออกมาต่างหาก เนื่องจากจะเป็นฐานข้อมูลที่มีขนาดใหญ่มาก	เป็นการทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลซึ่งทำเป็นรายกิจกรรม โดยมีรายละเอียดตามมาตรา 39
32	ในฐานะที่เป็นบริษัทที่ได้รับข้อมูลส่วนบุคคลของลูกค้า ข้อมูลส่วนบุคคลที่ได้รับมา จะเป็นกรรมสิทธิ์/ทรัพย์สินของบริษัทหรือไม่	ไม่เป็น

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

33	อยากทราบแนวทางการจัดการกับข้อมูล sensitive ในบัตรประชาชนที่ลูกค้าส่งมาโดยไม่ได้ขีดฆ่าปิดทึบ	อาจทำการขีดฆ่าปิดทึบเองหรือมีเทคโนโลยีอื่นใดที่จะทำการขีดฆ่าปิดทึบเพื่อให้ไม่ต้องเก็บข้อมูลส่วนบุคคลอ่อนไหวมาตั้งแต่แรก หรือหากเก็บมาแล้วก็ต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับข้อมูลส่วนบุคคลอ่อนไหว
34	PDPA check list ที่ อ.กล่าวถึง ใครกำหนด และอ้างอิงมาจากไหนครับ	หมายถึงการปฏิบัติตาม PDPA หรือไม่ สามารถดูแนวปฏิบัติเบื้องต้นได้ที่ TDPG 3.0 และดูสรุปผลของร่างกฎหมายลำดับรองทั้ง 3 กลุ่มได้ที่ https://www.law.chula.ac.th/event/10941/
35	ในส่วนขององค์กรจะต้องดำเนินการอย่างไร ในเรื่องของ ข้อมูลของพนักงาน เช่น จะต้องให้พนักงานลงชื่อยินยอมการใช้ข้อมูลของพนักงานเพื่อดำเนินการในการบริหารจัดการด้านข้อมูลภายในหรือไม่อย่างไร	ขึ้นอยู่กับกิจกรรมของบริษัท ไม่ได้มีบทตายตัวค่ะ ส่วนใหญ่ในกรณีนี้นายจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคล และเก็บรวบรวมข้อมูลส่วนตัวพนักงานตามฐาน contract อยู่แล้วค่ะ
36	ขอทิ้งคำถามไว้หน่อยครับ ถ้ามีการส่งข้อมูลส่วนบุคคลไปต่างประเทศควรมีการดำเนินการรองรับ PDPA อย่างไร	พิจารณาตามมาตรา 28 และ 29 รวมถึงร่างกฎหมายลำดับรองในส่วนที่เกี่ยวกับการโอนข้อมูลไปต่างประเทศ https://www.law.chula.ac.th/event/10941/
37	การนำข้อมูลลูกค้ามาทำ system testing จำเป็นต้องแจ้งให้ลูกค้าทราบก่อนหรือไม่ และต้องใช้ฐานทางกฎหมายอะไร และจะถือว่าการทำ system testing เป็นส่วนหนึ่งของวัตถุประสงค์ในการเปิดบัญชีลูกค้าได้หรือไม่	ไม่ว่าจะใช้ฐานทางกฎหมายใด ผู้ควบคุมข้อมูลส่วนบุคคลก็ต้องแจ้งรายละเอียดการประมวลผลให้เจ้าของข้อมูลทราบตามมาตรา 19 อาจจะเป็นฐานสัญญาและประโยชน์โดยชอบด้วยกฎหมายได้
38	ระหว่าง บลจ กับ ผู้สนับสนุนการขายหน่วยลงทุน ใครจะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล	ขึ้นอยู่กับกิจกรรมและการประมวลผลข้อมูลของบริษัท
39	ถ้าตอนแรกลูกค้าให้ความยินยอมเรียบร้อยแล้ว ต่อมาบริษัทมีการเปลี่ยน platform การให้บริการจากกระดาษ มาเป็น application แต่วัตถุประสงค์ในการประมวลผลเป็นอันเดิม แบบนี้ต้องขอความยินยอมใหม่มั้ยคะ ขอบคุณค่ะ	ต้องแจ้งการเปลี่ยนแปลงแพลตฟอร์มไปยังลูกค้า แต่ฐานการประมวลผลยังเป็นฐานเดิม

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

40	หากหน่วยงานกำกับดูแลของบริษัทแม่ในต่างประเทศ มีเกณฑ์กำหนดให้บริษัทแม่ต้องเปิดเผยข้อมูลบางอย่างของบริษัทลูกในประเทศไทย เพื่อการตรวจสอบกำกับดูแล โดยบริษัทลูกในประเทศจะต้องนำส่งข้อมูล ที่อาจมีข้อมูลของลูกค้า /พนักงาน ไปให้กับบริษัทแม่ตามการร้องขอ ในกรณีเช่นนี้ บริษัทลูกในไทย จะสามารถใช้ฐาน Legitimate interate ในการประมวลผลข้อมูล หรือ ต้องขอ Consent คะ	อาจเป็นฐานประโยชน์ด้วยชอบด้วยกฎหมายได้
41	กรณีลูกค้ามาขอแก้ไขข้อมูลส่วนบุคคลกับธนาคาร โดยเป็นการแก้ไขข้อมูลผลิตภัณฑ์ของธนาคารเอง และข้อมูลเกี่ยวกับผลิตภัณฑ์หน่วยลงทุนของบลจ (ธนาคารทำธุรกิจ LBDU ด้วย) ธนาคารต้องปฏิบัติอย่างไรในการทำการแก้ไขข้อมูลผลิตภัณฑ์หน่วยลงทุนของบลจ ตามที่ลูกค้าร้องขอ	ปฏิบัติตามปกติ แยกพิจารณาระหว่างแก้ไขข้อมูลกับแก้ไขวัตถุประสงค์
42	หากเก็บข้อมูลบัตรประชาชน และมี sensitive data เช่นศาสนา ควรจัดเก็บอย่างไร	ทำตามแนวทางที่ สคส.กำหนด
43	ข้อมูลที่เก็บไว้ก่อนกฎหมายประกาศใช้ เช่น ประวัติพนักงาน บริษัทต้องทำอย่างไร	ต้องพิจารณากิจกรรมก่อนว่าเป็นกิจกรรมอะไร ถ้าเกิดไม่ใช่กิจกรรมที่ต้องขอ consent ไม่ต้องมีการขอ consent แต่ถ้าเป็นฐาน consent ก็ต้องมีการขอใหม่ ต่อให้เคยขอ consent ไปแล้วก็ควรที่จะมีการขอใหม่เมื่อกฎหมายใช้บังคับเพราะบางทีการขอ consent เดิมอาจไม่ได้มาตรฐานตาม PDPA
44	จากกฎหมาย Consent จะทำเฉพาะ ข้อมูลอ่อนไหว ถูกต้องไหมครับ	การขอ consent จะไม่ได้ทำเฉพาะข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว ทั้งนี้ขึ้นอยู่กับวัตถุประสงค์ที่นำข้อมูลไปใช้โดยให้พิจารณาวัตถุประสงค์ตามมาตรา 26 หากไม่เข้ากรณีที่กำหนดไว้ ก็ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
45	ขอถามซักเล็กน้อยครับ เวลาร่าง policy ขึ้นมาต้องใช้ภาษากฎหมายหรือไม่ครับ	ขอให้นโยบายอ่านเข้าใจได้และถูกต้องตามกฎหมาย

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

46	Binding Corporate Rule มีความจำเป็นและมีประโยชน์ในแง่การคุ้มครอง ต่อบริษัทที่ต้องโอนข้อมูลไปยัง ตปท ให้กับ บริษัทในเครือมากน้อยเพียงใดคะ และหาก กฎหมาย PDPA บังคับใช้แล้วจะมีเกณฑ์/แนวทางการจัดทำ BCR ออกมาหรือไม่คะ	สามารถพิจารณาเกณฑ์เบื้องต้นได้ที่ร่างกฎหมายลำดับรองกลุ่มที่ 1 ที่ https://www.law.chula.ac.th/event/10941/
47	ในกรณีที่ขอเอกสารประกอบการสมัครงาน เช่น สำเนาบัตรประชาชน ใบจบการศึกษา โดยไม่มีการถ่ายเอกสารหรือเก็บไว้เพียงแค่ขอดูเป็นหลักฐานทั้งกรณี 1.ให้เค้าส่งมาทางอีเมลพร้อมเซ็นทับ 2.ให้เค้าถือมาในวันสัมภาษณ์แล้วให้นำกลับไป อยากทราบว่าต้องขอความยินยอมเป็นลายลักษณ์อักษรหรือไม่คะ หรือเพียงแค่บอกกล่าวก่อนขออย่างเดียว	การขอความยินยอมจะทำเป็นลายลักษณ์อักษรหรือด้วยวาจาก็ได้ ทั้งนี้ หากทำเป็นลายลักษณ์อักษรผู้ควบคุมข้อมูลก็จะมีหลักฐานเก็บไว้
48	PDPA มาตรา 39 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์	สามารถบันทึกได้ทั้งรูปหนังสือและอิเล็กทรอนิกส์
49	อย่างกรณีการสมัครงาน จะเห็นได้ว่า จำเป็นจะต้องใช้เอกสารประกอบการสมัครงาน เพื่อใช้พิจารณา ซึ่งในขั้นตอนดังกล่าว ควรจะต้องให้มีการลงชื่อยินยอมของผู้สมัครหรือไม่ เพื่อมิให้เกิดปัญหาในภายหลัง	การสมัครงานอาจเป็นฐานสัญญาเพราะจำเป็นต่อการขอเข้าทำสัญญาคือให้พิจารณาคุณสมบัติเพื่อเข้าเป็นพนักงาน
50	เราจะ identify ระดับชั้นของข้อมูล pii ใดบ้างที่ต้อง encryption คะ เช่น การส่งไฟล์ข้ามทีม (ภายในออฟฟิศเดียวกัน) ต้อง encrypt ด้วยหรือไม่ค่ะ	เป็นไปตามความเสี่ยงและนโยบายของแต่ละองค์กร

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

51	ขออนุญาตสอบถามครับ ถ้าบริษัทแม่มีบริษัทลูกและบริษัทในเครือจำนวนหลายบริษัท แต่ใช้บุคลากรของบริษัทแม่ร่วมกัน เช่น HR เป็นต้น ในการดำเนินงานงานซึ่งข้อมูลทั้งหมดจะถูกจัดเก็บที่บริษัทแม่ (ไม่ใช่บริษัทในเครือ) ในกรณีเช่นนี้ บริษัทต้องจัดให้มี privacy compliance program แยกไปตามแต่บริษัท หรือสามารถทำแค่บริษัทแม่เพียงบริษัทเดียวก็เพียงพอแล้วครับ	เพื่อความชัดเจนหรือกรณีมีรายละเอียดที่แตกต่างกันบางจุดในแต่ละบริษัทในเครือก็อาจจะทำแยกเป็นบริษัทตัวเองก็ได้
52	Vendor ที่เอาเอกสารในถุงแดงไปทำลาย ถือเป็น data processor หรือไม่ ต้องมีสัญญา รับผิด หรือ nda หรือไม่ อย่างไร	การจะเป็นผู้ประมวลผลหรือไม่ต้องพิจารณาว่าสามารถเข้าถึง แก้ไข หรือทำการใดๆกับข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุม หากทำลายเฉยๆโดยไม่ทราบถึงข้อมูลต่างๆก็ไม่เป็นผู้ประมวลผล
53	DPO ปัจจุบันมาจากพนักงานภายในองค์กร อยากทราบว่า ปัจจุบันส่วนใหญ่มาจากฝ่ายไหนครับ HR/IT/LAW ขอบคุณครับ	ขึ้นอยู่กับโครงสร้างองค์กร ทั้งนี้ หน้าที่หลัก 4 ข้อของ DPO คือ 1. ให้คำแนะนำ 2. ตรวจสอบ 3. ประเมินความเสี่ยง 4. ประสานงานกับคณะกรรมการ ฯ โดยต้องมีความรู้เรื่อง PDPA และรู้ business operation ว่าข้อมูลในองค์กรเป็นอย่างไรบ้าง และอาจจะมีส่วนที่เกี่ยวกับงาน IT ด้วย และเนื่องจาก DPO เป็น second-line of defense คล้ายกับ compliance ฝ่ายสนับสนุนจึงอาจสามารถมาจากฝ่ายกฎหมาย IT หรือ compliance แต่ไม่ควรใช้คนจาก first-line of defense เพื่อป้องกันการขัดกันของผลประโยชน์
54	อยากให้อ.แนะนำ คุณสมบัติที่เหมาะสม สำหรับคนที่จะทำหน้าที่ DPO มีบางคำแนะนำบอกว่าไม่ควรให้ผู้บริหารระดับ C Level มาเป็น DPO ซึ่งสำหรับบริษัทที่ไม่ได้มีพนักงานจำนวนมาก หรือหลายระดับควรจะเป็นใครคะ	DPO สามารถจัดตั้งเป็นบุคคลบุคคลเดียวหรือคณะทำงานก็ได้ โดยคุณสมบัติของ DPO กฎหมายไม่ได้กำหนดไว้เป็นการเฉพาะ แต่ละบริษัทสามารถพิจารณาได้ด้วยตนเองตามความเหมาะสม อาจจะตั้งเป็นคณะทำงานแล้วมีตำแหน่งสูงสุดเป็นคนตัดสินใจสุดท้ายก็ได้

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

55	ถ้าข้อมูลถูกบันทึกลงระบบ ERP หรือระบบขนาดใหญ่อื่นๆ ที่เวลาสั่งให้ delete มันจะเป็นแค่ soft delete คือข้อมูลถูก mark ไม่ให้เข้าถึงได้แต่ไม่ได้ลบไปจริงๆ เพราะมันผูกกับข้อมูลชุดอื่นอยู่ ในกรณีอย่างนี้บริษัทจะต้องทำอย่างไรให้ถูกต้องตามกฎหมายครับ (ทำ anonymization หรือ pseudonymization หรือ modify ระบบเองไม่ได้เพราะเป็นระบบสำเร็จรูปจากต่างประเทศ)	บริษัทก็ต้องบันทึกไว้เป็นหลักฐานถึงขั้นตอนในการลบหรือทำลายข้อมูล
56	ในกลุ่มธุรกิจสถานพยาบาลที่มีบริษัทย่อยเป็นการทำธุรกิจเกี่ยวกับสุขภาพ ที่อาจต้องเปิดเผยข้อมูลระหว่างกัน เช่น ข้อมูลสุขภาพ ฯลฯ ควรต้องมีการทำสัญญาเกี่ยวกับความลับและข้อมูลส่วนบุคคลกันระหว่างบริษัทด้วยหรือไม่	ควร เพื่อหน้าที่ที่ชัดเจนและบันทึกไว้เป็นหลักฐาน
57	ทำไมคนเสียชีวิตไม่ถือเป็นข้อมูลส่วนบุคคล	พิจารณาคำนิยามตามมาตรา 6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
58	การติดตั้งกล้องวงจรปิดละเมิดข้อมูลส่วนบุคคลหรือไม่	ต้องพิจารณาวัตถุประสงค์ในการติดตั้งกล้องวงจรปิด ต้องอธิบายได้ว่าเก็บข้อมูลไปเพื่ออะไร เช่น เพื่อประโยชน์โดยชอบด้วยกฎหมายในการรักษาความปลอดภัย ทั้งนี้ ควรมีการแจ้งถึงการติดตั้งกล้องวงจรปิดไว้ในบริเวณดังกล่าวให้เจ้าของข้อมูลทราบได้
59	กรณีการให้บริการซึ่งต้องใช้ sensitive data จะใช้สัญญาหรือ consent คะ	กรณีข้อมูลอ่อนไหวหรือ sensitive data ให้พิจารณาวัตถุประสงค์ตามมาตรา 26 หากไม่เข้ากรณีที่กำหนดไว้ ก็ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

60	กรณีบริษัทมี website แต่จ้าง outsource เป็นผู้ดูแลจัดทำการ website ให้ มีประเด็นว่า ข้อมูลการเข้าใช้งาน เช่น IP Address เบราว์เซอร์ที่ใช้งานของเจ้าของข้อมูล ออกไปสู่บุคคลที่ 3 ซึ่งบุคคลที่ 3 ในที่นี้จะหมายถึงการติดตั้ง Google analytic ซึ่งทาง Google จะต้องเป็นผู้เห็นข้อมูลเช่นเดียวกัน เนื่องจากเป็นผู้ให้บริการในส่วนของ Analytic ที่ทางบริษัทผู้ให้บริการได้ทำการติดตั้งไป หรืออาจหมายถึงพวก script ต่างๆ ที่มีการเขียนใช้งาน Cookie ก็ถือเป็นบุคคลที่ 3 เช่นเดียวกัน ขอสอบถามว่า สามารถระบุข้อความนี้ในนโยบายของบริษัทได้หรือไม่ “บริษัทไม่สามารถควบคุมการใช้ข้อมูลของบุคคลที่สามนั้นได้ นโยบายความเป็นส่วนตัว (Privacy Notice) และนโยบายการใช้คุกกี้ของบุคคลที่สาม ซึ่งแตกต่างจากเว็บไซต์ของบริษัท เราได้ที่เว็บไซต์ของบุคคลที่สามนั้น ๆ” หรือควรดำเนินการอย่างไร ขอบคุณค่ะ	อาจจะระบุให้ชัดเจนยิ่งขึ้นว่าบุคคลที่สามที่บริษัทจะเปิดเผยข้อมูลให้ได้แก่บริษัทใดบ้าง
61	ทางหน่วยงานราชการ มีเอกสารที่เป็นนโยบาย PDPA เบื้องต้น ที่บริษัทต่างๆจะสามารถนำไปใช้เป็นพื้นฐานในการดำเนินการหรือไม่ อย่างไรครับ ถ้ามี รบกวนขอด้วยครับ ขอบคุณมากครับ	สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) ได้จัดทำเอกสารแม่แบบสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลภาครัฐ https://www.dga.or.th/document-sharing/article/59030/
62	สำหรับแบบฟอร์มการใช้สิทธิ์ของลูกค้า ตาม PDPA นั้น มีตัวอย่างเพื่อให้บริษัทได้ดูหรือไม่คะ	สคส. ไม่ได้จัดทำตัวอย่างแบบฟอร์ม ท่านสามารถศึกษาตัวอย่างของ สพร. หรือ TDPG ที่จัดทำโดยคณะนิติศาสตร์ จุฬาฯ
63	ขอทราบความคืบหน้ากฎหมายลำดับรองสำหรับการส่งข้อมูลไปต่างประเทศ และประเทศที่มีความคุ้มครองเทียบเท่าครับ	ท่านสามารถศึกษาเพิ่มเติมได้จาก เอกสารผลการรับฟังความเห็นเกี่ยวกับ (ร่าง) กฎหมายลำดับรอง กลุ่มที่ 1 เรื่องกำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

*** *คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม*****

		https://www.mdes.go.th/mission/82 หัวข้อ ผลการศึกษาภายใต้โครงการของสำนักงานฯ
64	กรณีบริษัทมีการขายของ Online ซึ่งในการส่งสินค้าให้ทางลูกค้า จะต้องมีการเปิดเผย ชื่อ นามสกุล ที่อยู่ และเบอร์โทรศัพท์ของลูกค้า ซึ่งเป็นการดำเนินการส่งสินค้าตามปกติ ถือเป็นการเปิดเผยข้อมูลส่วนตัวหรือไม่ และบริษัทควรจะต้องมีมาตรการอย่างไรหรือไม่คะ	บริษัทผู้ขายสินค้าเป็นผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งได้รับข้อมูล
65	การเผยแพร่ข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กรณีเป็นหน่วยงานของรัฐจำเป็นต้องมีการประกาศเป็นทางของหน่วยงานของรัฐ หรือต้องจัดทำเป็นประกาศเผยแพร่ผ่านราชกิจจานุเบกษาหรือไม่	คุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลในการแจ้งรายละเอียด หน่วยงานอาจเผยแพร่ประกาศแต่งตั้ง DPO เพิ่มเติมก็ได้
66	การแจ้ง data breach จะมีแบบฟอร์มหรือ requirement ไหมครับว่าต้องแจ้งรายละเอียดเรื่องอะไรบ้าง	ท่านสามารถศึกษาเพิ่มเติมได้จาก เอกสารผลการรับฟังความเห็นเกี่ยวกับ (ร่าง) กฎหมายลำดับรอง กลุ่มที่ 1 เรื่องการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล https://www.mdes.go.th/mission/82 หัวข้อ ผลการศึกษาภายใต้โครงการของสำนักงานฯ
67	ถ้าบริษัทแต่งตั้ง DPO เป็นคณะบุคคล เวลาแจ้งชื่อให้ สคส. ต้องแจ้งชื่อทุกท่าน ไหมครับ	เนื่องจากมาตรา 41 กำหนดว่า เจ้าของข้อมูลส่วนบุคคลต้องสามารถติดต่อ DPO เกี่ยวกับการใช้สิทธิตามกฎหมายฉบับนี้ ดังนั้น DPO ควรเป็นชื่อของบุคคลที่ได้รับมอบหมายให้ติดต่อประสานงานกับเจ้าของข้อมูลส่วนบุคคลและ สคส.
68	กรณีบริษัทจำกัดทั่วไปซึ่งเป็นบริษัทเล็กๆ มีพนักงานจำนวนจำกัด อยู่ในบังคับภายใต้กฎหมายนี้ หรือไม่ และหากอยู่ภายใต้กฎหมายนี้ แนวปฏิบัติของบริษัทสามารถยืดหยุ่นอย่างไรได้บ้าง	ท่านสามารถศึกษาเพิ่มเติมได้จาก เอกสารผลการรับฟังความเห็นเกี่ยวกับ (ร่าง) กฎหมายลำดับรอง กลุ่มที่ 1 เรื่อง การจัดให้มีบันทึกรายการกิจกรรมประมวลผล https://www.mdes.go.th/mission/82 หัวข้อ ผลการศึกษาภายใต้โครงการของสำนักงานฯ

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

69	จากที่คุณสุนทรีย์ได้ present มาแสดงว่าหากเกิดเหตุละเมิด แจ้งให้อีเมล์ดังกล่าวใช่หรือไม่คะ	e-mail แจ้งชื่อ DPO และ Data Breach : pdpc.dpo@mdes.go.th
70	ข้อมูลในสถาบันการศึกษา เกี่ยวกับ ข้อมูลนักศึกษา ผู้สอน ซึ่งมีข้อมูล sensitive อยู่ในนั้น แต่จะมีกรณีที่มีผู้ประกอบการ ขอข้อมูล นักศึกษาไปเพื่อพิจารณาการเข้าไปทำงาน ซึ่ง มหาวิทยาลัยเคยให้ไปแล้ว แต่ปรากฏว่าข้อมูล นักศึกษาถูกเอาให้อีกหลายๆบริษัท ในกรณี มหาวิทยาลัยควรทำอย่างไรครับ	ต้องพิจารณาว่า สถาบันการศึกษาเปิดเผยข้อมูลของนักศึกษาแก่ผู้ประกอบการโดยใช้ฐานการประมวลผลใด หากเป็นความสัมพันธ์แบบผู้ควบคุมข้อมูลส่วนบุคคล 2 ฝ่ายแบ่งปันข้อมูลส่วนบุคคลและนำไปใช้ตามวัตถุประสงค์ของตนเอง ควรจัดทำข้อตกลงแลกเปลี่ยนข้อมูลส่วนบุคคลที่กำหนดวัตถุประสงค์ของการแลกเปลี่ยนและขอบเขตความรับผิดของแต่ละองค์กรให้ชัดเจน
71	กรณีเป็นบริษัทผลิต จำนวนลูกค้าไม่มากเท่า โลตัส การบินไทย ธนาคารฯ ควรต้องทำอย่างไรครับ?	ท่านสามารถศึกษาข้อมูลได้จาก https://www.mdes.go.th/mission/82 หัวข้อ เอกสารเผยแพร่ประชาสัมพันธ์
72	ขอรายชื่อหน่วยงานหรือบุคคลของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่จะให้คำแนะนำและคำปรึกษา ที่สามารถติดต่อได้ทางโทรศัพท์ หรือ email ด้วยค่ะ	fb page : PDPC Thailand e-mail สอบถามข้อมูล : pdpc@mdes.go.th

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

ลำดับ	คำถาม	คำตอบ
กรณีเกิดเหตุข้อมูลรั่วไหล		
1	แล้วสรุปว่าการบินไทยโดนปรับไหมครับ ในกรณีที่ข้อมูลที่รั่วไหลจากบริษัทฯ	ในกรณีที่ข้อมูลที่รั่วไหลจากบริษัทฯ 1) หลายประเทศมีคำสั่งแจ้งปิดคดี โดยมีประเทศหนึ่งให้เหตุผลว่าเนื่องจากเห็นว่าเป็นกรณีของความผิดพลาดที่เกิดจากบุคคล ซึ่งมิใช่ระบบ ซึ่งอาจจะเกิดจากความเหนื่อยล้าและ ความวิตกกังวล และได้มีการแก้ไขเหตุการณ์ที่จำเป็นแล้ว อีกทั้งข้อมูลไม่ได้มีลักษณะที่ก่อให้เกิดความเสียหายแก่บุคคล 2) มีการแจ้งข้อแนะนำที่จำเป็น เช่น ก) การเยียวยาความเสียหาย ในขั้นตอนการสอบสวน ข) การใช้ระบบเข้ามาช่วยเพื่อการตรวจสอบความถูกต้อง ค) ตรวจสอบกระบวนการเป็นระยะๆ เพื่อให้มีความทันสมัยต่อวัตถุประสงค์ ง) สุ่มตรวจพนักงานในการปฏิบัติตามนโยบายและกระบวนการ และความถูกต้องของข้อมูล จ) ประเมินความเสี่ยงแก่ข้อมูลที่ได้รับผลกระทบ ฉ) ทำการอบรมพนักงานอย่างสม่ำเสมอทุกๆ 2 ปีโดยใช้กรณีนี้เป็นกรณีศึกษา 3) เนื่องจากปัญหา Covid-19 อาจมีพนักงานบางส่วนไม่ได้ปฏิบัติงานอย่างเต็มรูปแบบ จึงขอให้ดำเนินการตามมาตรการที่แนะนำโดยเร็วที่สุด เท่าที่เป็นไปได้ ส่วนกรณีที่เกิดจากบุคคลที่ 3 บุคคลที่ 3 เป็นผู้รายงาน เรามิได้เป็นผู้รายงาน
2	อยากให้ทางบริษัท share template กรณีมีเหตุรั่วไหลด้วยได้ไหมคะ	ดูที่ slide presentation ของ ดร. สิทธินัย (การบินไทย)
3	สคส จะมีการออก คำนิยาม หรือ หลักเกณฑ์ ที่เรียกว่า การละเมิดข้อมูลส่วนบุคคล /ข้อมูลรั่วไหลที่เข้าข่าย ที่ต้องรายงาน สคส ตามมาตรา 37 (4) ซึ่งหากมีการละเมิดฯ ต้อง รายงานภายใน 72 ชั่วโมง	ท่านสามารถศึกษาเพิ่มเติมได้จาก เอกสารผลการรับฟังความเห็นเกี่ยวกับ (ร่าง) กฎหมายลำดับรอง กลุ่มที่ 1 https://www.mdes.go.th/mission/82 หัวข้อ ผลการศึกษาภายใต้โครงการของสำนักงานฯ
4	กรณีมีการจ้างบ.Cloud ดูแลเกิดการรั่วไหล โดนโจมตี ที่บ.Cloud ที่เราจ้าง ทางบ.ขอคำแนะนำว่าจะรองรับด้วยวิธีการแบบใดได้บ้างคะ	มาตรา 40 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานของผู้ประมวลผลข้อมูลให้เป็นไปตามกฎหมาย

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****

5	หลังจากทราบว่าข้อมูลรั่วไหล การส่งเมลแจ้งเจ้าของข้อมูล และ หน่วยงานกำกับที่เกี่ยวข้องจะต้องรอให้ IT ดำเนินการ Forensic ก่อนหรือไม่ และใช้เวลากี่วันในการทำ Forensic	ต้องรอจนกว่าจะทราบแน่นอนว่ามีการรั่วไหลเกิดขึ้น ซึ่งในกรณีที่รายงานค่อนข้างแน่ชัด เนื่องจากมีลูกค้าส่งเมลตอบกลับมาว่า มิใช่เอกสารที่เป็นชื่อของตน และจากการตรวจสอบอย่างละเอียดว่ามีความผิดพลาดแน่นอน จึงเริ่มกระบวนการในการรายงาน ซึ่งใช้เวลาค่อนข้างน้อย เมื่อลูกค้ารายงานมา มีการตรวจสอบ ก็สามารถทราบได้ในเวลาอันรวดเร็ว แต่ใช้พนักงานในการตรวจสอบอย่างละเอียด หลายท่านในเวลาติดต่อกัน จนกว่าจะทราบผล ส่วนสำหรับกรณีบุคคลที่สาม เป็นกรณีที่ทางผู้ทำข้อมูลรั่วไหลได้รายงานการรั่วไหลมาแล้ว เราก็จะดำเนินการโดยเร็วที่สุด
		1.เจ้าของข้อมูลส่วนบุคคล - ทางบริษัททำการแจ้งเมื่อเกิดเหตุการณ์โจมตีทางไซเบอร์ เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล 2.กรณีพบว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ทางบริษัทควรต้องแจ้ง**<u>หน่วยงานกำกับด้านการคุ้มครองข้อมูลส่วนบุคคลในเบื้องต้น โดยไม่ต้องรอผลสรุปจาก Forensic</u>** จากนั้นเมื่อได้รับข้อมูลรายละเอียดเพิ่มเติมจาก Forensic จึงทำการนำส่งเพิ่มเติมในภายหลัง ระยะเวลาการทำ Forensic ขึ้นกับขอบเขตของการถูกโจมตี ปริมาณ/ความซับซ้อนของข้อมูลที่ถูกละเมิด และหลักฐานทางดิจิทัล และผลการวิเคราะห์หลักฐานทางดิจิตอลที่ได้รับจากการตรวจสอบแล้วแต่กรณี จึงไม่สามารถกำหนดกรอบระยะเวลาที่แน่นอนได้
6	จากกรณีของ Bangkok airways หลังจากถูกโจมตี ส่วนของข้อมูล ได้มีการแจ้งเจ้าของข้อมูล ภายใน 72 ชม. อย่างไรบ้างครับ	บริษัททำการแจ้งข้อมูลแก่เจ้าของข้อมูลผ่านช่องทางดังต่อไปนี้ 1.e-mail 2.website และ Facebook ของทางบริษัท 3.สื่อสาธารณะ

**** คำตอบที่แสดงเป็นความเห็นของวิทยากรในการตอบคำถามจากการจัดงานสัมมนา ซึ่งหากนำไปใช้อาจต้องดูกฎหมายและบริบทที่เกี่ยวข้องเพิ่มเติม****