คำถามจากสัมมนา เรื่อง PDPA กับการจัดการตาม ISO/IEC 27701

คำถาม	แสดงความเห็นตามข้อซักถาม
1. ขอทำความเข้าใจ Definition ของ "การละเมิด" ค่ะ	ตาม ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 (มีผลใช้บังคับเมื่อวันที่ 15 ธันวาคม 2565) "การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดย ปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่นใด
2. เรื่องการขอ consent หากเรามีการแจ้งเจ้าของข้อมูลวัตถุประสงค์การเก็บข้อมูล ก็ไม่จำเป็นต้องส่ง consent letter ให้เขาอนุญาตกลับถูกต้องไหมคะ ขอบคุณค่ะ	การขอ consent คือการขอความยินยอม กับเจ้าของข้อมูลตามกฎหมาย การแจ้ง consent และการแจ้งวัตถุประสงการเก็บ ควร เป็นไปตาม "แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (เผยแพร่เมื่อวันที่ 7 กันยายน 2565)" และ "แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (เผยแพร่เมื่อวันที่ 7 กันยายน 2565)" ครับ
3. ข้อมูลส่วนบุคคลที่อ่อนไหว(Sensitive Personal Data) ต้องใช้ฐานการประมวลผล Consent เท่านั้นใช่หรือไม่ครับ ไม่สามารถใช้ฐานอื่นๆได้ใช่ไหมครับ	ไม่เสมอไปครับ ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ (๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม (๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กร ที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น (๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

คำถาม	แสดงความเห็นตามข้อซักถาม
	(๕) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของ ลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติ ตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่ รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของ ข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่อ อันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพ ของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือ ตามจริยธรรมแห่งวิชาชีพ (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับ การรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูล ส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐาน และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการ ที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการ ประกาศกำหนด (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครอง สิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
4. การเก็บบัตรประชาชน สามารถเก็บสำเนา ที่ฝ่าย HR ได้กี่ใบคะ รวมถึง เอกสารต่างๆเช่นทะเบียนบ้าน	องค์กรจะเก็บข้อมูลส่วนบุคคล จะต้องกำหนด วัตถุประสงค์การเก็บครับ ว่าเก็บเอาไปทำอะไร และการ copy ไปต่อนั้นจำเป็นแค่ไหม อย่างไรครับ ต้องขึ้นกับวัตถุประสงค์
5. อยากให้อาจารย์อธิบายนิยาม PII และการจัดทำ ค่ะ ขอบคุณค่ะ	PII (personally identifiable information) – คือข้อมูลส่วนบุคล (“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ)
6. ถ้า C.7 กับ C.8 อ้างอิง GDPR สามารถเข้าใจได้ไหมคะว่า หากทำ ISO 27701 แล้วเรา align ตาม PDPA ของไทย หรือเราต้องทำอะไรเพิ่มเติมไหมคะ	ทำ ISO 27701 ไม่ได้บอกว่า เราจะ comply กับ PDPA ข้อกำหนด ISO 27701 (6, 7, 8) align กับ PDPA การ Implement ตาม ISO 27701 ต้อง นะ PDPA มา implement ด้วยตามข้อ 5.2, 6.15
7. กรณีของกล้องวงจรปิด ต้องทำป้าย ไหมคะ ว่าบริเวณนี้มีกล้อง วงจรปิด ติดป้ายเป็นสัญลักษณ์ ให้รับทราบอะคะ	การติดกล้อง ไว้ที่บ้าน หรือในรถ ไม่จำเป็นต้องขอ ตามที่ Facebook PDPC Thailand แนะนำ ครับ

คำถาม	แสดงความเห็นตามข้อซักถาม
	การติดกล้องที่ ตึกสำนักงาน ควรแจ้งให้ ผู้เกี่ยวข้องทราบ ครับ
8. เวลาทำขอยกเว้น บางข้อกำหนดของ 27701 ได้หรือไม่คะ เช่น บริการของเราไม่มีเก็บข้อมูลส่วนบุคคล ออกไปต่างประเทศ (clause 7.5 PII sharing, transfer and disclosure) / ขอบคุณค่ะ	สามารถทำได้ครับ ใช้หลักการ Risk approach เหมือน ISO 27001 ได้เลยครับ การเลือก หรือไม่เลือก Control ใดๆ ตามข้อ 6, 7, 8 ต้องกำหนด ใน SOA และต้องแจ้ง เหตุผลใน SOA ด้วยครับ
9. มีหนังสือหรือคู่มือ (ที่มีการรวบรวม) ที่พาทำเป็นลำดับขั้นตอนตั้งแต่ต้นจนจบบ้างไหมครับ	สามารถ ใช้มาตรฐาน ISO27701 ได้เลยครับ
10. ในการเข้าตลาดหลักทรัพย์ จะอ้างอิง PDPA อย่างไรได้บ้างคะ หรือ เอกสาร ที่ต้องทำ สำหรับ pdpa มา ปรับใช้ แต่ละฝ่าย ในบริษัท ในการเริ่มเข้าตลาดหลักทรัพย์ อยากได้เป็นความรู้คะ	องค์กร จะเข้า ตลาดหลักทรัพย์ หรือไม่ หากอยู่ในประเทศต้อง comply ข้อกำหนด PDPA ครับ โดย เรา ต้องศึกษา กฎหมาย ใน website ของ PDPC Thailand ครับ ข้อมูลในนั้น มีประโยชน์ ช่วยเราได้ตรับ
11. ขอชื่อประกาศของ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับการ certify ของ 27701 หน่อยค่ะ / ขอบคุณค่ะ	ในlink นี้ได้เลยครับ https://www.mdes.go.th/mission/detail/2319