ประเด็นคำถาม – คำตอบ : แนวปฏิบัติเรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline)

คำถาม	ความเห็น/ คำตอบ
๑. ขอบเขตการบังคับใช้	แนวปฏิบัติฉบับนี้ จัดทำขึ้นโดยมุ่งหวังให้บริษัทประกันภัยนำไปประยุกต์ใช้เป็นแนวทางอ้างอิงเพื่อดำเนินการเรื่อง การกำกับดูแลข้อมูล (Data Governance) และบริหารจัดการข้อมูลภายในองค์กร อย่างไรก็ตาม ผู้ประกอบธุรกิจที่มิใช่บริษัทประกันภัย เช่น บริษัทนายหน้าประกันภัย เป็นต้น สามารถพิจารณาแนวปฏิบัติฉบับนี้ในการอ้างอิงหรือประยุกต์ใช้ เพื่อดำเนินการในเรื่อง การกำกับดูแลข้อมูลได้ตามความเหมาะสม
๒. ความเชื่อมโยงหรือทับซ้อนกับกฎระเบียบที่เกี่ยวข้อง เช่น ประกาศและแนวปฏิบัติเรื่อง IT Risk Management เป็นต้น	แนวปฏิบัติฉบับนี้ จัดทำขึ้นโดยพิจารณาให้มีความเชื่อมโยงกับข้อกำหนดในประกาศ คปภ. ว่าด้วยหลักเกณฑ์การกำกับดูแล และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. ๒๕๖๓ ซึ่งกำหนดให้ทุกบริษัทต้องมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในส่วนที่เกี่ยวข้องกับข้อมูลด้วย โดยจะครอบคลุมในเรื่องบริหารจัดการทรัพย์สินสารสนเทศของบริษัท เช่น การจัดทำทะเบียนทรัพย์สินสารสนเทศ (ข้อมูล ฮาร์ดแวร์ และซอฟแวร์) กำหนดแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลสอดคล้องตามชั้นความลับ การควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ การเข้ารหัสข้อมูล (Cryptography) ที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูล การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่างๆ และการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ อย่างไรก็ตาม แนวปฏิบัติฉบับนี้จะให้แนวทาง ตัวอย่าง รวมทั้งข้อเสนอแนะในการดำเนินการเชิงรายละเอียด ขยายความจากประกาศในมุมของการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลเพิ่มเติมจากเรื่องการรักษาความมั่นคงปลอดภัย เพื่อเป็นแนวทางให้บริษัทประกันภัยนำไปพิจารณาดำเนินการ
๓. ระยะเวลาในการบังคับใช้ หรือระยะเวลาที่ให้บริษัทในการเตรียมความพร้อม หากแนวปฏิบัติฉบับนี้ยกระดับขึ้นมาเป็นประกาศที่มีผลบังคับทางกฎหมาย	แนวปฏิบัติฉบับนี้เป็น Soft Law ซึ่งเป็นส่วนขยายความที่ให้รายละเอียดในทางปฏิบัติในการกำกับดูแลข้อมูลที่สอดคล้องกับประกาศ คปภ. ว่าด้วยหลักเกณฑ์การกำกับดูแล และบริหารจัดการ

คำถาม	ความเห็น/ คำตอบ
	ความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. ๒๕๖๓ ในเบื้องต้น สำนักงานมีความเห็นว่า บริษัทสามารถอ้างอิงแนวปฏิบัติในการเริ่มต้นเพื่อดำเนินการ เรื่อง การกำกับดูแล และบริหารจัดการข้อมูลภายในองค์กร เพื่อให้ส่วนที่ต้องอาศัยระยะเวลาในการดำเนินการ หรือการเริ่มต้นจัดให้มีขึ้น ซึ่งตรงนี้จะช่วยให้บริษัทมีระยะเวลาในพัฒนา และดำเนินการปรับปรุงคุณภาพได้อย่างต่อเนื่อง อย่างไรก็ตาม การออกประกาศหรือกฎระเบียบของสำนักงาน คปภ. จะมีการทำ public hearing อีกครั้ง ซึ่งเป็นขั้นตอนปกติที่สำนักงานดำเนินการในปัจจุบัน ส่วนหนึ่งเพื่อรับฟังความคิดเห็น และข้อเสนอแนะของทุกบริษัท รวมทั้งประเด็นปัญหาหรืออุปสรรคในการดำเนินการตามประกาศฯ เพื่อนำมาพิจารณาความเหมาะสมของกฎระเบียบต่างๆ ที่จะบังคับใช้กับบริษัท รวมทั้งระยะเวลาในการบังคับใช้ และความพร้อมของบริษัทในการปฏิบัติตามซึ่งเป็น Key หลักสำคัญที่สำนักงานจะนำมาพิจารณาประกอบ
๔. การมอบหมายหน้าที่ความรับผิดชอบให้คณะกรรมการชุดย่อย (Sub-Committee) ดำเนินการในเรื่อง Data Governance รวมทั้ง การกำหนดองค์ประกอบของคณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee)	แนวปฏิบัติฉบับนี้ กำหนดให้คณะกรรมการบริษัทมีหน้าที่ความรับผิดชอบ ในการกำกับดูแลให้บริษัทดำเนินการ ด้านที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ให้เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อน และความเสี่ยงด้านข้อมูลของบริษัท รวมทั้งสอดคล้องกับกลยุทธ์ทางธุรกิจ ทั้งนี้ คณะกรรมการบริษัทสามารถมอบหมาย **ให้คณะกรรมการชุดย่อยที่มีอยู่แล้วในปัจจุบัน (หมายความรวมถึงคณะกรรมการชุดย่อยที่บริษัทมีการแต่งตั้งทั้งตามที่กฎหมายกำหนด หรือนอกเหนือจากที่กฎหมายกำหนด)** หรือ **พิจารณาจัดตั้งคณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) ขึ้นมาใหม่เป็นการเฉพาะ** ก็ได้ ซึ่งในส่วนนี้จะเปิดให้ขึ้นกับดุลยพินิจของคณะกรรมการบริษัทในการพิจารณามอบหมายโดยหลักการแล้ว ควรพิจารณาบทบาทหน้าที่ และ ความรับผิดชอบที่ต้องดำเนินการในส่วนที่เกี่ยวข้องแก่คณะกรรมการชุดย่อยที่ได้รับการมอบหมาย รวมทั้งความเหมาะสมหรือความพร้อมในด้านอื่น

คำถาม	ความเห็น/ คำตอบ
	ประกอบ เช่น ความรู้ ความเข้าใจ องค์ประกอบของกรรมการในคณะกรรมการชุดย่อย เป็นต้น อย่างไรก็ตาม องค์ประกอบของคณะกรรมการชุดย่อย Data Governance Committee แนวปฏิบัติฉบับนี้ ยังไม่ได้มีการกำหนดเป็นข้อบังคับเกี่ยวกับองค์ประกอบของคณะกรรมการ แต่จัดทำไว้ให้เป็นคำแนะนำในเบื้องต้น เพื่อให้บริษัทนำไปใช้เป็นแนวทางประกอบการพิจารณากำหนดองค์ประกอบของ Data Governance Committee ของบริษัทต่อไป ทั้งนี้ ในมุมของกรรมการบริษัทที่จะมาทำหน้าที่ใน Data Governance Committee ต้องเป็นกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศด้วยหรือไม่นั้น สำนักงานมีความเห็นว่า ในกรณีที่บริษัทมีความพร้อม รวมทั้งมีกรรมการที่มีความรู้ประสบการณ์ด้าน IT แล้ว และสามารถลงมาทำหน้าที่ในการกำกับดูแลการดำเนินงานของคณะกรรมการชุดย่อยนี้ด้วยตัวเอง ถือว่าเป็นสิ่งที่ดี นอกจากเป็นการสร้าง Tone from the Top ที่ชัดเจนแล้ว ยังเป็นการสร้าง linkage ในการทำงานระหว่าง Data Governance Committee และ Board of Director ด้วย
๕. หน้าที่การปฏิบัติตามกฎหมาย และหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล สำหรับกรณีที่บริษัทมีการแต่งตั้ง Compliance และ DPO ทั้ง ๒ ส่วนงานนี้จะทำหน้าที่เป็น 2nd line ใช่หรือไม่	ใช่ กล่าวคือ Compliance และ DPO ทำหน้าที่ใน 2nd line of defense ซึ่งตามหลักการ 3 line of defense หน่วยงาน Compliance จะเป็นส่วน 2nd line ทำหน้าที่ facilitate ให้หน่วยงานภายในองค์กรเกี่ยวกับเรื่องการปฏิบัติตามกฎหมายและติดตามการออกกฎหมายหรือประกาศใหม่ ซึ่งในส่วนนี้จะครอบคลุมกฎหมาย ประกาศ หรือกฎระเบียบทุกเรื่องที่บริษัทต้อง comply ทั้งหมด ทั้งนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) มีหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดขององค์กร รวมทั้งให้คำปรึกษา ตรวจสอบ กำกับดูแลการใช้ข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะมีความเฉพาะเจาะจงในรายละเอียดของเรื่องข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายที่เกี่ยวข้องว่าด้วยเรื่องข้อมูลส่วนบุคคล

คำถาม	ความเห็น/ คำตอบ
๖. เรื่องการรักษาความเป็นส่วนบุคคลของข้อมูล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จะทำหน้าที่เป็น 2nd line ดังนั้น หน้าที่ของ Data Governance Committee รวมทั้ง คณะทำงานที่ปฏิบัติหน้าที่ด้านบริกรข้อมูล (Data Steward) ถือเป็น 1st line ซึ่งต้องกำหนดนโยบาย และแนวทางการบริหารจัดการข้อมูลทั้งหมดในภาพรวม โดยมี DPO กำกับดูแล และให้คำแนะนำ เพื่อให้การกำหนดนโยบาย และแนวทางปฏิบัติในการจัดการข้อมูลเป็นไปตามที่ PDPA กำหนด ตามหลัก 3 line of defense ใช่หรือไม่	Data Governance Committee หรือคณะทำงานที่เกี่ยวข้องใน แนวปฏิบัติฉบับนี้ มุ่งหวังให้ทำหน้าที่กำกับดูแล และบริหารจัดการข้อมูลทุกประเภทในองค์กร ซึ่งในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล คณะกรรมการชุดนี้สามารถปรึกษา รวมทั้งขอคำแนะนำ หรือความเห็นจาก DPO ของบริษัทได้ เพื่อสามารถดำเนินการได้อย่างถูกต้องครบถ้วนตามที่กฎหมายกำหนด ทั้งนี้ ตามหลักการ 3 line of defense ส่วนของ 1st line และ 2nd line สามารถทำงานร่วมกันหรือประสานงานกันได้ รวมทั้งบริษัทสามารถพิจารณาให้ DPO มาเป็นหนึ่งในกรรมการของคณะกรรมการ Data Governance Committee ของบริษัทได้ เพื่อช่วยในการกำกับดูแลในเรื่องข้อมูลส่วนบุคคล
๗. กรณีที่บริษัทฯ มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPA Steering Committee) หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอยู่แล้วในปัจจุบัน บริษัทควรกำหนดหน้าที่ในเรื่องการรักษาความเป็นส่วนบุคคลของข้อมูลให้กับบุคลากรสองชุดดังกล่าวข้างต้น หรือควรมอบหมายให้คณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) กำกับดูแลในเรื่องนี้ด้วย	เบื้องต้นหน้าที่ความรับผิดชอบของคณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) มุ่งหวังให้ดำเนินการกำกับดูแลและบริหารจัดการข้อมูลทุกประเภทขององค์กร ซึ่งรวมถึงข้อมูลส่วนบุคคลด้วย อย่างไรก็ตาม คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPA Steering Committee) หรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลทั้งหมดขององค์กร รวมทั้งให้คำปรึกษา ตรวจสอบ กำกับดูแลการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะมีความเฉพาะเจาะจงในรายละเอียดของเรื่องข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมายที่เกี่ยวข้องว่าด้วยเรื่องข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติ เห็นว่า บุคลากรสองกลุ่มนี้สามารถพิจารณาดำเนินงานร่วมกันได้ในการกำกับดูแลและบริหารจัดการในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
๘. ความเชื่อมโยงของคณะกรรมการ Data Governance Committee กับ คณะกรรมการ IT Steering Committee และ Risk Management Committee	คณะกรรมการ IT Steering Committee (1st line) มีหน้าที่ในการกำกับดูแลและบริหารจัดการด้านการใช้งานเทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ ในส่วนของคณะกรรมการ Data Governance Committee (2nd line) มีหน้าที่กำกับดูแลและบริหารจัดการในเรื่องของข้อมูลทั้งหมดขององค์กร เช่น การกำหนดนโยบายการบริหารจัดการข้อมูล คุณภาพของข้อมูล การบริหาร

คำถาม	ความเห็น/ คำตอบ
	จัดการข้อมูลสำคัญหรือข้อมูลส่วนบุคคล ปริมาณของข้อมูล เป็นต้น และคณะกรรมการ Risk Management Committee (2nd line) จะทำหน้าที่กำกับดูแลการบริหารจัดการความเสี่ยงในภาพรวมทั้งหมดขององค์กร ซึ่งรวมถึงความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีและข้อมูล เช่น ความเสี่ยงจากข้อมูลส่วนบุคคลรั่วไหล และ ความเสี่ยงจากภัยทางไซเบอร์ เป็นต้น ซึ่งคณะกรรมการทั้ง 3 ชุดนี้ สามารถ integrate การทำงานในภาพรวม โดยสามารถแลกเปลี่ยนข้อมูลหรือประสานงานร่วมกันได้ในส่วนที่เกี่ยวข้อง
๙. ความเชื่อมโยงเกี่ยวกับบทบาทหน้าที่ของคณะกรรมการกำกับดูแลข้อมูล กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	- วัตถุประสงค์ของคณะกรรมการชุดย่อยทั้ง 2 มีความแตกต่างกันดังนี้ **คณะกรรมการกำกับดูแลข้อมูล** มีหน้าที่รับผิดชอบงานด้านการกำกับดูแลการบริหารจัดการข้อมูล เพื่อที่บริษัทสามารถใช้ประโยชน์จากข้อมูลที่อยู่บนพื้นฐานของ ข้อมูลที่มีคุณภาพ ถูกต้อง ครบถ้วน มั่นคงปลอดภัย และมีความเป็นส่วนบุคคล ผ่าน**กระบวนการกำกับดูแลข้อมูล (Data Governance)** และ **การบริหารจัดการข้อมูล (Data Management)** ตลอดทุกช่วงวงจรชีวิตของ**ทุกข้อมูล**ที่สำคัญต่อการดำเนินงานภายในองค์กร โดยที่ไม่ได้จำกัดเพียงเฉพาะข้อมูลลูกค้าหรือผู้เอาประกันภัยเท่านั้น **คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล** มีหน้าที่รับผิดชอบการบริหารจัดการการได้มาของข้อมูล การเก็บรักษา และปกป้อง **ข้อมูลของลูกค้าและผู้เอาประกันภัย** ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การกำกับดูแลและบริหารจัดการข้อมูลจึงมีลักษณะเป็นภาพใหญ่และครอบคลุมหัวข้อการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ซึ่งเป็นหนึ่งในหัวข้อย่อยของกระบวนการกำกับดูแลและบริหารจัดการข้อมูล วัตถุประสงค์ของทั้งสองคณะกรรมการชุดย่อยจึงมีความแตกต่างกันและไม่สามารถทดแทนกันได้ตามที่ได้กล่าวไปข้างต้น

คำถาม	ความเห็น/ คำตอบ
	อย่างไรก็ดี ทั้งสองคณะกรรมการมีความสัมพันธ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าและผู้เอาประกันภัย คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจึงสามารถมีบทบาทหน้าที่ในการให้คำแนะนำและสนับสนุนคณะกรรมการกำกับดูแลข้อมูลในการปฏิบัติหน้าที่เพื่อคุ้มครองข้อมูลส่วนบุคคลของลูกค้าและผู้เอาประกันภัยได้
๑๐. - Business Data Steward ควรเป็นคนเดียวกัน หรือ ควรรวมความรับผิดชอบเป็น role เดียวกันกับ Data Owner เพื่อไม่ให้เกิดความซับซ้อน และขาดประสิทธิภาพในทางปฏิบัติ - Data Steward ควรได้รับการแต่งตั้งจาก Data Owner เพราะ Data owner โดยหน้าที่มักจะเป็นหัวหน้าหน่วยงานหรือแผนก และ data owner สามารถ assign บุคคลที่มีความรู้ความสามารถที่เกี่ยวกับ business หรือการใช้ Data ของหน่วยงานตนตัวเอง	- โดยทั่วไปแล้ว Business Data Steward และ Data Owner จะเป็นคนละ level กัน เช่น Data Owner จะเป็นระดับบริหาร และมีอำนาจในการตัดสินใจเกี่ยวกับข้อมูลชุดนั้นๆ เช่น ผู้อำนวยการฝ่าย และสำหรับ Data Steward จะเป็นระดับคนทำงานที่มีความเข้าใจและเชี่ยวชาญเรื่องข้อมูลในฝ่ายงานของตนเอง เป็นต้น อย่างไรก็ตามในทางปฏิบัติจริงบริษัทสามารถพิจารณาปรับใช้ได้ตามความเหมาะสมกับบริบทขององค์กร - การแต่งตั้งหรือมอบหมายการทำหน้าที่เป็น Data Steward เห็นด้วย ว่าควรเป็น Data Owner ที่เป็นหัวหน้าหน่วยงานทำการแต่งตั้งหรือมอบหมายให้บุคลากรที่เหมาะสมทำหน้าที่เป็น Data Steward อย่างไรก็ตาม ในส่วนนี้ยังเปิดให้แต่ละบริษัทสามารถใช้ดุลยพินิจในการพิจารณากำหนดหรือมอบหมายบุคลากรมาเป็น Data Steward ได้ตามความเหมาะสมและ ความพร้อมในด้านที่เกี่ยวข้อง
๑๑. การสื่อสารเกี่ยวกับการบริหารจัดการข้อมูลให้กับผู้ที่เกี่ยวข้องทราบอย่างทั่วถึง รวมทั้งบุคลากรทุกระดับในองค์กร เห็นควรเพิ่มผู้ให้บริการจากภายนอกด้วย	เห็นด้วย ในกรณีนี้บริษัทสามารถพิจารณาเพิ่มเติมในส่วนของการสื่อสาร และระเบียบวิธีปฏิบัติเกี่ยวกับผู้ให้บริการภายนอกได้ตามความเหมาะสม
๑๒. นโยบายควรครอบคลุม ข้อมูลทุกประเภท ซึ่งรวมถึงข้อมูลส่วนบุคคล และไม่ว่าจะมีการจัดเก็บในรูปแบบใด เช่น กระดาษ อิเล็กทรอนิกส์ เสียง ใช่หรือไม่	ใช่ ทั้งนี้ แนวทางในการดำเนินการ คำแนะนำ หรือตัวอย่างในแนวปฏิบัติฉบับนี้ มุ่งเน้นข้อมูลที่เป็นอิเล็กทรอนิกส์ และข้อมูลที่อยู่ในระบบเป็นหลัก (Digital Files) อย่างไรก็ตาม บริษัทสามารถพิจารณาดำเนินการเพิ่มเติมให้ครอบคลุมเหมาะสมกับข้อมูลแต่ละประเภทที่อยู่ในรูปแบบที่แตกต่างกันได้ตามความเหมาะสม
๑๓. โครงสร้างการกำกับดูแลข้อมูลสำหรับบริษัทประกันภัยในแต่ละกลุ่มบริษัทขนาดเล็ก กลาง และใหญ่	แนวปฏิบัติฉบับนี้ จัดทำขึ้นเพื่อให้บริษัทนำไปประยุกต์ใช้เป็นแนวทางอ้างอิงในการกำกับดูแล และบริหารจัดการข้อมูลภายในองค์กร ในเบื้องต้นรายละเอียดต่างๆ ในแนวปฏิบัติฉบับนี้จะให้

คำถาม	ความเห็น/ คำตอบ
	ข้อมูลที่เป็นพื้นฐานสำคัญในการสร้างให้เกิดการทำเรื่อง data governance โดยบริษัทสามารถพิจารณาตามความเหมาะสมและปรับใช้ได้ตามบริบทขององค์กรตามเหตุผลความจำเป็นในส่วนที่ต้องดำเนินการ
๑๔. แนวทางการตรวจสอบการดำเนินการของบริษัทตามแนวปฏิบัติ เรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline)	หลังจากที่แนวปฏิบัติได้มีการเผยแพร่เพื่อให้บริษัทดำเนินการ ในส่วนของการดำเนินการเข้าตรวจสอบ สำนักงานจะกำหนดแนวทางเพื่อเข้าตรวจสอบการดำเนินการในเรื่องดังกล่าวต่อไป
๑๕. เสนอแนะเพิ่มขั้นตอน (ก่อนขั้นตอนการทำลายข้อมูล) “การจัดเก็บข้อมูล (Archive) คือ การทำสำเนาสำหรับการเก็บรักษาข้อมูลที่ไม่ได้ใช้งานแล้ว แต่ยังไม่เกินกว่าระยะเวลาจัดเก็บที่กำหนด เพื่อนำกลับไปใช้งานได้ใหม่เมื่อต้องการ”	ปรับแก้ไขเพื่อความชัดเจน โดย ๒) การจัดเก็บข้อมูล (Store) คือ การจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือจัดเก็บข้อมูลให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหายหรือถูกทำลาย และผู้ใช้งานสามารถประมวลผลข้อมูลตามความต้องการได้อย่างรวดเร็ว โดยสามารถดำเนินการได้ทั้งในรูปแบบการลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) และรวมถึงการจัดเก็บข้อมูลถาวร เพื่อทำสำเนาสำหรับการรักษาโดยข้อมูลนั้นไม่มีการลบ ปรับปรุง แก้ไข และสามารถนำกลับไปใช้งานใหม่ได้ เมื่อต้องการใช้งาน
๑๖. การบริหารจัดการวงจรชีวิตของข้อมูล โดยส่วนใหญ่จะมีความเกี่ยวข้องกับนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล และการรักษาความเป็นส่วนบุคคลของข้อมูลอยู่แล้ว เห็นควรอ้างอิงถึงข้อกำหนดที่เกี่ยวข้องต่างๆ เพื่อให้การดำเนินการบริหารจัดการข้อมูลให้มีความสอดคล้องกัน	เพื่อเป็นการลดความซ้ำซ้อนในการกำกับดูแลในเรื่องที่เกี่ยวข้อง แนวปฏิบัติฉบับนี้ ได้อ้างอิงกฎระเบียบ หรือประกาศที่เกี่ยวข้องไว้แล้ว ดังนี้ - การรักษาความมั่นคงปลอดภัยของข้อมูล ให้บริษัทดำเนินการตามที่ประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. ๒๕๖๓ และ แนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. ๒๕๖๔ - การรักษาความเป็นส่วนบุคคลข้อมูล ให้บริษัทปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง เช่น พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือ ประกาศสำนักงาน คปภ. เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประชีวิต/วินาศภัย พ.ศ. ๒๕๖๔ เป็นต้น อย่างไรก็ตาม เพื่อให้บริษัทสามารถมั่นใจว่า ได้ดำเนินการอย่างครบถ้วน และเป็นไปตามที่ประกาศของสำนักงาน หรือ

คำถาม	ความเห็น/ คำตอบ
	กฎหมายที่เกี่ยวข้องที่บริษัทต้องปฏิบัติตามกำหนดครบถ้วนแล้ว บริษัทสามารถประสานงานหรือขอคำปรึกษาเพิ่มเติมได้จากหน่วยงาน Compliance ของบริษัทได้
๑๗. ขอเสนอให้คำอธิบายข้อมูลเชิงเทคนิค เป็นตัวเลือก เนื่องจากระบบสำเร็จบางระบบในตลาดทางผู้ขายอาจจะไม่ได้ให้รายละเอียดเชิงลึกถึง Technical Metadata และบริษัทที่ซื้อระบบสำเร็จมาใช้งานอาจไม่สามารถทำเอกสารเชิงเทคนิคนี้เองได้	การจัดทำคำอธิบายข้อมูลทั้งในเชิงธุรกิจและเชิงเทคนิค บริษัทควรพิจารณาให้ครอบคลุมชุดข้อมูลสำคัญที่จำเป็นต้องมีคุณภาพ (Critical Data Element) ในการดำเนินธุรกิจ โดยอย่างน้อยควรพิจารณา ข้อมูลที่เกี่ยวข้องกับการดำเนินงานด้านการรับประกันภัย (Underwriting) และงานด้านการบริหารจัดการค่าสินไหมทดแทน (Claims Management) เนื่องจากข้อมูลดังกล่าวมีความสำคัญในการให้บริการผู้เอาประกันภัย การพิจารณารับประกันภัย รวมถึงการปฏิบัติตามภาระผูกพันที่มีต่อผู้เอาประกันภัย
๑๘. เสนอให้เพิ่มเติมคำว่า Validity แทนคำว่า Relevancy	ในแนวปฏิบัติฉบับนี้ คำว่า Data relevancy มุ่งหวังให้บริษัทดำเนินการประเมินว่าข้อมูลตรงตามวัตถุประสงค์และความต้องการใช้งานของผู้ใช้ข้อมูลหรือไม่ เช่น ในการพัฒนาผลิตภัณฑ์และการบริการควรเก็บรวบรวมข้อมูลที่เป็นประโยชน์แก่การวิจัยและพัฒนาในเรื่องดังกล่าว และควรพิจารณาลดทอนหรือตัดข้อมูลที่ไม่จำเป็นหรือไม่เกี่ยวข้องแก่การวิจัยออก เพื่อให้บริหารต้นทุนในด้านการพัฒนาผลิตภัณฑ์ และการบริการมีประสิทธิภาพมากขึ้น เป็นต้น ดังนั้น ความหมายของคำว่า Data relevancy จึงมีความแตกต่างจากการทำ Data accuracy หรือ Data Consistency ที่พิจารณาความถูกต้องและ Format ของข้อมูล รวมทั้งคำว่า Data availability จะหมายถึง ให้บริษัทมีการประเมินคุณภาพของข้อมูลในด้านข้อมูลมีความพร้อมใช้งานอยู่เสมอ อย่างไรก็ตาม แนวทางการประเมินคุณภาพข้อมูลตามแนวปฏิบัติฉบับนี้ เป็นเพียงแนวทางในเบื้องต้นเพื่อช่วยเพิ่มความเร็วและเห็นภาพชัดเจนขึ้นในสิ่งที่ต้องดำเนินการสำหรับบริษัทที่ปัจจุบันอาจยังไม่มีการดำเนินการในส่วนนี้ โดยสามารถใช้อ้างอิงและนำไปประยุกต์ใช้ในการกำกับดูแลและบริหารจัดการข้อมูลได้อย่างเหมาะสมตามลักษณะ ขนาด และความซับซ้อนของบริษัท หรือสำหรับบริษัทที่มีการดำเนินการในส่วนนี้อยู่แล้ว สามารถนำมาเป็นข้อมูลประกอบการพิจารณาทบทวน หรือปรับปรุงแนวทางในการ

คำถาม	ความเห็น/ คำตอบ
	ประเมินคุณภาพของข้อมูลที่ใช้อยู่แล้วในปัจจุบันเพิ่มเติมได้ ดังนั้น ในการกำหนดปัจจัยเพื่อมาทำเกณฑ์ในการประเมินคุณภาพของข้อมูล บริษัทสามารถพิจารณาเพิ่มหรือลดปัจจัยที่จะนำมากำหนดเป็นเกณฑ์ในการประเมินคุณภาพของข้อมูลได้ตามความเหมาะสม จากตัวอย่างหรือคำแนะนำในแนวปฏิบัติฉบับนี้
๑๙. หลักเกณฑ์ที่อ้างถึง ๒.๓.๔ (๑) หมายถึงหลักเกณฑ์เรื่องอะไร	หลักเกณฑ์ในข้อนี้ จะหมายถึง หลักเกณฑ์ในการประเมินคุณภาพของข้อมูล
๒๐. ความเสี่ยงของข้อมูล รวมถึงความถูกต้องครบถ้วน แต่ควรระวังเรื่องการเข้าไปแก้ไขข้อมูลด้วยเช่นกัน เนื่องจากการแก้ไขข้อมูลไม่ได้มีการกล่าวถึงในหัวข้ออื่นๆ ในร่างปฏิบัติก่อนหน้า เนื่องจากส่วนนี้เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูล อาจจะเพิ่มเติมข้อกำหนดเกี่ยวกับการแก้ไขข้อมูลลงไป มีการกำหนดระยะเวลาในการเก็บข้อมูล เพื่อให้ทราบถึงความเสี่ยง และ scale of risk ที่อาจจะเกิดขึ้น	บริษัทสามารถพิจารณาแนวทางตามประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ในการกำกับดูแล และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย และแนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทฯ จะมีกล่าวถึงเรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) ในหัวข้อการควบคุมการเข้าถึงข้อมูล หรือระบบ (access control) และการบริหารจัดการทรัพย์สินสารสนเทศ (asset management) เพื่อให้สามารถระบุชุดข้อมูลที่สำคัญที่ต้องมีการควบคุมทั้งด้านการใช้งาน การเข้าถึง การแก้ไข การส่งต่อ หรืออื่นๆ รวมทั้งสามารถกำหนดแนวทางในการบริหารจัดการความเสี่ยงที่เหมาะสมกับประเภทของข้อมูล และระดับชั้นความลับของข้อมูล ซึ่งรวมถึงข้อมูลส่วนบุคคลด้วย
๒๑. - เสนอให้มีการกำหนดขั้นต่ำในการเข้ารหัสข้อมูลเพื่อป้องกันข้อมูลสารสนเทศได้อย่างปลอดภัย - การเข้ารหัสข้อมูลควรกำหนดด้วยว่าข้อมูลชนิดใดควรเข้ารหัสทั้งในขณะเก็บข้อมูล และ / หรือ ในระหว่างเรียกดู (in rest and in transit) กำหนด technology ว่าจะใช้อะไรในการเข้ารหัส เช่น WinZIP ควรประกาศใช้ให้ชัดเจน (เช่น version อะไร จะได้ไม่มีปัญหาในรายละเอียด) และต้องสนับสนุนด้วย เรื่องค่าใช้จ่ายของ software หรือเปิดให้ download ฟรี	ในประเด็นนี้ ขอให้บริษัทพิจารณาเทคนิค หรือเทคโนโลยีในการเข้ารหัสข้อมูลได้ตามความเหมาะสม เนื่องจากการกำหนดหรือระบุเครื่องมือที่ชี้ชัดลงไป อาจจะทำให้มีผลกระทบกับบริษัทอื่นที่ปัจจุบันมีความแตกต่างกันทั้งในด้านความพร้อม ความรู้ความเข้าใจบุคลากร และต้นทุนในการจัดหา ดังนั้น ในบางเรื่องสำนักงานจะพิจารณากำหนดในลักษณะเป็นมาตรฐานขั้นต่ำตามหลักการ Principle base เพื่อให้มีการดำเนินการในเรื่องนี้ แต่วิธีการหรือเทคนิคที่จะใช้เพื่อให้การดำเนินการของบริษัทเป็นไปตามที่กฎหมายกำหนดหรือไม่นั้น รวมถึงการพิจารณาว่าข้อมูลชุดไหนควรเข้ารหัสอย่างไร สำนักงานเปิดให้บริษัทใช้วิจารณญาณพิจารณาได้ตามความ

คำถาม	ความเห็น/ คำตอบ
	เหมาะสม หรือความเสี่ยงของชุดข้อมูลตามที่บริษัทกำหนด ตามหลักการ Proportionality อย่างไรก็ตาม การเข้ารหัสข้อมูลกับชุดข้อมูลที่ต้องเข้ารหัสขอให้คำนึงถึงข้อกำหนดในประกาศ คปภ. และแนวปฏิบัติ ว่าด้วยหลักเกณฑ์ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย ที่กำหนดให้บริษัทต้องจัดให้มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล (Cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับ และความสำคัญของข้อมูลสารสนเทศ
๒๒. แนวทางป้องกันข้อมูลที่สำคัญและอ่อนไหว “การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล โดยประเมินความเสี่ยงจากการระบุแหล่งที่จัดเก็บข้อมูลที่สำคัญและอ่อนไหว และแนวทางการป้องกันที่ใช้อยู่ในปัจจุบันว่ามีความสอดคล้องและเหมาะสมเพียงพอกับความเสี่ยง “	แนวทางในการบริหารจัดการและป้องกันข้อมูลที่สำคัญและอ่อนไหวเบื้องต้นบริษัทสามารถพิจารณาดำเนินการได้ โดยการจัดทำรายการทะเบียนทรัพย์สินข้อมูล (Data Inventory) เพื่อให้ทราบว่าบริษัทมีการจัดเก็บข้อมูลสำคัญ หรือใช้งานในปัจจุบันไว้ที่ใดหรือระบบใดบ้าง ทราบเจ้าของข้อมูล สามารถกำหนดแนวทางควบคุมการเข้าถึงได้เหมาะสมสอดคล้องกับความสำคัญของข้อมูล และระดับชั้นความลับของข้อมูล เพื่อให้ข้อมูลเหล่านี้ได้รับการป้องกันหรือเข้ารหัสที่สอดคล้องกับชั้นความลับอย่างเหมาะสม รวมทั้งมีการกำหนดนโยบายหรือแนวปฏิบัติที่ชัดเจน และสื่อสารให้ผู้เกี่ยวข้องทราบหรือเพื่อให้การปฏิบัติกับข้อมูลที่สำคัญหรืออ่อนไหวได้อย่างถูกต้อง ซึ่งส่วนนี้จะช่วยกำหนดขอบเขตของการกำกับดูแล และดูเรื่องความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลสำคัญแลอ่อนไหวได้ชัดเจนมากขึ้น อย่างไรก็ตาม บริษัทสามารถพิจารณาเพิ่มเติมได้จากมาตรฐานต่างๆ ที่เกี่ยวข้อง เช่น การบริหารจัดการความมั่นคงปลอดภัยข้อมูล ตามมาตรฐาน ISO/IEC 27001:2013 เป็นต้น
๒๓. นโยบาย Data Security Policy ควรครอบคลุมเรื่องอะไรบ้าง และความถี่ในการทบทวน	นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล ควรพิจารณากำหนดให้สอดคล้องกับการนำข้อมูลมาใช้ในการดำเนินธุรกิจ และความเสี่ยงที่อาจเกิดขึ้นจากการใช้ข้อมูล และต้องสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ของบริษัท รวมทั้งหลักการ CIA

คำถาม	ความเห็น/ คำตอบ
	ทั้งนี้ บริษัทสามารถพิจารณาจัดทำนโยบายให้ครอบคลุมในเรื่องดังต่อไปนี้ - ขอบเขตของการรักษาความมั่นคงปลอดภัยของข้อมูล - การปฏิบัติตามกฎหมายที่เกี่ยวข้อง - กรอบการดำเนินงานด้านการรักษาความปลอดภัยของข้อมูลภายในบริษัท - หน้าที่ความรับผิดชอบของบุคลากรภายในบริษัทที่มีต่อการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งนี้ ความถี่ในการทบทวนนโยบายดังกล่าว สามารถพิจารณาให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) หลักของบริษัท หรืออย่างน้อยปีละหนึ่งครั้ง หรือทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ ซึ่งอาจส่งผลกระทบต่อการบริหารและจัดการข้อมูล
๒๔. - การระบุคุณสมบัติของเครื่องมือ และความรู้ของบุคคลากรในการกำกับดูแลและบริหารจัดการข้อมูลให้ชัดเจน เนื่องจากเป็นปัจจัยที่มีผลต่อเกณฑ์ในการประเมินระดับการกำกับดูแลข้อมูลของบริษัท - การกำหนดคุณสมบัติขั้นต่ำ หรือประสบการณ์ที่จำเป็นของตำแหน่งต่างๆ เช่น หัวหน้าบริกรข้อมูล(Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Steward) และบริกรข้อมูลด้านเทคนิค (Technical Data Steward)	เห็นด้วยกับการกำหนดคุณสมบัติของเครื่องมือ และคุณสมบัติหรือประสบการณ์ของบุคลากรที่เกี่ยวข้องในการกำกับดูแลและบริหารจัดการข้อมูล ในเบื้องต้น สำนักงานขอรับประเด็นดังกล่าวไว้เป็นข้อมูลประกอบการพิจารณาปรับเกณฑ์ให้เข้มข้นขึ้นต่อไปในอนาคต อย่างไรก็ตาม เรื่อง Data Governance สำหรับ บริษัทประกันภัยส่วนใหญ่ อาจจะอยู่ในช่วงเริ่มต้นดำเนินการ โดยแนวทางที่สำนักงานใช้ผลักดันในเรื่องนี้ ช่วงเริ่มต้นจะให้บริษัทดำเนินการจัดโครงสร้างองค์กร กำหนดผู้รับผิดชอบหรือดำเนินการอย่างชัดเจน รวมทั้งกำหนดนโยบายและแนวทางปฏิบัติที่เกี่ยวข้องให้ครอบคลุมการบริหารจัดการข้อมูล ซึ่งในหลายส่วนต้องใช้เวลาในการพัฒนาและดำเนินการอย่างต่อเนื่องเพื่อสร้างให้เกิดขึ้นโดยเฉพาะอย่างยิ่งการพัฒนาบุคลากร ซึ่งแนวปฏิบัติฉบับนี้ ได้ให้ความสำคัญในการสร้างความรู้ความเข้าใจให้กับบุคลากรทุกระดับในองค์กรที่เหมาะสมตามบทบาทหน้าที่ความรับผิดชอบ รวมทั้งได้รับการจัดสรรทรัพยากรและงบประมาณ เพื่อรองรับการดำเนินการและมีเครื่องมือเพียงพอที่จะสนับสนุนการปฏิบัติงานที่เกี่ยวข้องในการกำกับดูแลข้อมูลต่อไป ซึ่งการกำหนดเกณฑ์ในการ

คำถาม	ความเห็น/ คำตอบ
	คัดกรองเครื่องมือหรือคุณสมบัติบุคลากรทันทีในช่วงเริ่มต้น อาจจะยังไม่เหมาะสมกับบริษัทประกันภัยส่วนใหญ่ในภาพรวม
๒๕. - การกำหนดผู้รับผิดชอบในการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment) ความถี่ในการประเมินและการรายงานผลการประเมิน - การประเมิน Data Maturity Assessment ในระดับองค์กรใครควรเป็นคนตอบแบบสอบถามหรือทำในระดับทีมแล้วค่อยรวบรวมขึ้นมาเป็นระดับภาพรวมขององค์กร	แนวปฏิบัติฉบับนี้ ไม่ได้ระบุหรือกำหนดเป็นการเฉพาะ ทั้งในเรื่องผู้รับผิดชอบที่ต้องทำหน้าที่ในการประเมินระดับการกำกับดูแลข้อมูล ความถี่ในการประเมิน และการรายงานผลการประเมิน ดังนั้น บริษัทสามารถพิจารณามอบหมายบุคลากรที่มีศักยภาพเพื่อดำเนินการในส่วนนี้ได้ตามความเหมาะสม รวมทั้งการกำหนดรอบความถี่ในการประเมิน และการรายงานผลไปยัง ผู้ที่เกี่ยวข้อง อย่างไรก็ตาม วัตถุประสงค์ของการประเมินระดับการกำกับดูแลข้อมูล เพื่อให้บริษัททราบถึงสถานะของระดับการกำกับดูแลข้อมูลที่บริษัทดำเนินการอยู่ในปัจจุบัน และสามารถนำผลที่ได้มาเป็นข้อมูลประกอบการพิจารณาพัฒนาแนวทาง การบริหารจัดการข้อมูลให้ได้ตามระดับ Maturity ที่บริษัทตั้งเป้าหมายไว้ได้ นอกจากนี้ รอบความถี่ในการประเมินระดับการกำกับดูแลข้อมูลสามารถพิจารณาทำเป็นประจำทุกปีได้ เพื่อให้เห็นความคืบหน้าในการดำเนินการ หรืออาจใช้เป็นเครื่องมือในการติดตามประสิทธิภาพของการดำเนินการได้ สำหรับการรายงานผลการประเมิน บริษัทสามารถรายงานไปยัง ผู้ที่เกี่ยวข้องที่มีหน้าที่ในการกำกับดูแล หรือดำเนินการในเรื่อง นี้ได้ เช่น คณะกรรมการบริษัท คณะกรรมการชุดย่อยที่ได้รับมอบหมาย เป็นต้น
๒๖. ระดับ Maturity ในการกำกับดูแลข้อมูลของบริษัทที่สำนักงาน คปภ. คาดหวัง	ระดับ Maturity ของการกำกับดูแลข้อมูลของบริษัท สำนักงานมุ่งหวังให้มีการดำเนินการที่สอดคล้องกับขนาด ลักษณะ ความเสี่ยง และความซับซ้อนในการดำเนินธุรกิจของบริษัท
๒๗. การประเมินระดับ Maturity สามารถดำเนินการเองได้ หรือ require third party/vendor เข้ามาทำ Maturity assessment	การดำเนินการประเมินระดับ Data Governance Maturity Assessment สามารถพิจารณาดำเนินการเองได้ หรือกรณีที่บริษัทต้องการผลการประเมินที่โปร่งใส และสามารถสะท้อนภาพความจริงของการดำเนินการในเรื่องนี้ สามารถพิจารณาจัดจ้างผู้เชี่ยวชาญที่มีความเป็นอิสระมาดำเนินการในส่วนนี้ได้
๒๘. การประเมินประสิทธิผลในการบริหารจัดการข้อมูล บริษัทต้องนำส่งสำนักงาน คปภ. หรือไม่ และความถี่ในการจัดส่งเป็นอย่างไร	สำนักงานไม่ได้กำหนดให้บริษัทต้องนำส่งเอกสาร แต่ในแนวปฏิบัติฉบับนี้จะระบุให้บริษัทพิจารณาดำเนินการกำกับดูแลและบริหารจัดการเรื่องข้อมูลตามที่กำหนด

คำถาม	ความเห็น/ คำตอบ
๒๙. บริษัทฯ มีการกำหนดแนวทางการประเมินระดับ การกำกับดูแลข้อมูลไว้ในนโยบาย และสามารถเพิ่มเกณฑ์ และรายละเอียดทางการประเมินระดับการกำกับดูแลข้อมูลไว้ในเอกสารมาตรฐานการกำกับดูแลข้อมูลได้หรือไม่	บริษัทสามารถพิจารณาดำเนินการได้

กลุ่มงานมาตรฐานธรรมาภิบาลและการดำเนินธุรกิจ

สายพัฒนามาตรฐานการกำกับ สำนักงาน คปภ.