แนวปฏิบัติตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการ

ฉบับปรับปรุง ตุลาคม 2566

คำนำ

เอกสารแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการฉบับนี้ จัดทำขึ้นเพื่อให้สถานประกอบการที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน ได้นำไปใช้เพื่อประกอบการดำเนินกิจกรรมของสถานประกอบการที่เกี่ยวกับข้อมูลส่วนบุคคลของบุคลากรให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เอกสารฉบับนี้จะเกิดขึ้นมิได้ หากไม่ได้รับการสนับสนุนจาก นายนิยม สองแก้ว อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย ที่ปรึกษาคณะทำงาน และความร่วมแรงร่วมใจจากคณะทำงานของกรมสวัสดิการและคุ้มครองแรงงาน รวมไปถึงหน่วยงานที่เกี่ยวข้องที่ทำให้เกิดเอกสารฉบับนี้ โดยเฉพาะอาจารย์สุกฤษ โกยอัครเดช, อาจารย์สันต์ภพ พรวัฒนะกิจ, อาจารย์มยุรี ชวนชม, อาจารย์ดวงดาว สำนองสุข รวมถึงท่านอื่น ๆ ที่มิได้เอ่ยนามมา ณ ที่นี้

ด้วยเงื่อนไขของเวลาและข้อจำกัดทางกฎหมายที่ได้มีการเริ่มประกาศใช้ หากท่านมีข้อสังเกต ข้อแลกเปลี่ยนความคิดเห็น ตลอดจนข้อติชมต่าง ๆ หรือหากมีข้อผิดพลาดประการใด สามารถแนะนำได้ที่ pdpasme@smethai.or.th และสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ www.smethai.or.th/pdpasme เพื่อที่จะนำมาใช้ในการปรับปรุงและพัฒนาเอกสารแนวปฏิบัติการคุ้มครองแรงงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ให้เป็นประโยชน์กับทุกฝ่ายต่อไป

กรมสวัสดิการและคุ้มครองแรงงาน

สมาพันธ์เอสเอ็มอีไทย

PDPA Thailand

สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

20 กรกฎาคม 2565

คำนำ (แก้ไขเพิ่มเติมครั้งที่ 2)

ในโอกาสครบรอบ 1 ปีของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งฉบับซึ่งได้มีกฎหมายลำดับรองประกาศตามมาอีกหลายฉบับ จึงได้ดำเนินการแก้ไขเพิ่มเติมเอกสารแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการฉบับนี้ โดยการเพิ่มเติมเนื้อหาคำอธิบายรวม เพื่อให้มีความชัดเจน ครบถ้วน บริบูรณ์มากขึ้น ตลอดจนสอดคล้องกับกฎหมายลำดับรองที่เกี่ยวข้อง ทำให้ผู้ที่สนใจและสถานประกอบการที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน ได้นำไปปรับใช้ประกอบการดำเนินกิจกรรมที่เกี่ยวกับข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เอกสารฉบับนี้จะเกิดขึ้นมิได้ หากไม่ได้รับการสนับสนุนจาก นายนิยม สองแก้ว อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย ที่ปรึกษาคณะทำงาน และความร่วมแรงร่วมใจจากคณะทำงานของกรมสวัสดิการและคุ้มครองแรงงาน รวมไปถึงหน่วยงานที่เกี่ยวข้องที่ทำให้เกิดเอกสารฉบับนี้ โดยเฉพาะอาจารย์สุกฤษ โกยอัครเดช, อาจารย์สันต์ภพ พรวัฒนะกิจ, อาจารย์มยุรี ชวนชม, อาจารย์ดวงดาว สำนองสุข รวมถึงท่านอื่น ๆ ที่มิได้เอ่ยนามมา ณ ที่นี้

หากท่านมีข้อสังเกต ข้อแลกเปลี่ยนความคิดเห็น ตลอดจนข้อติชมต่าง ๆ หรือหากมีข้อผิดพลาดประการใด สามารถแนะนำได้ที่ pdpasme@smethai.or.th และสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ www.smethai.or.th/pdpasme เพื่อที่จะนำมาใช้ในการปรับปรุงและพัฒนาเอกสารแนวปฏิบัติการคุ้มครองแรงงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ให้เป็นประโยชน์กับทุกฝ่ายต่อไป

กรมสวัสดิการและคุ้มครองแรงงาน

สมาพันธ์เอสเอ็มอีไทย

PDPA Thailand

สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

20 กรกฎาคม 2566

คำนำ (แก้ไขเพิ่มเติมครั้งที่ 3)

ในโอกาสครบรอบ 1 ปีของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งฉบับ ซึ่งได้การแก้ไขเพิ่มเติมครั้งที่ 2 แล้ว ต่อมา ได้มีกฎหมายลำดับรองที่สำคัญประกาศออกมาเพิ่มเติม จึงได้ดำเนินการแก้ไขเพิ่มเติมเอกสารแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการฉบับนี้ โดยการเพิ่มเติมเนื้อหาคำอธิบาย เพื่อให้มีความชัดเจน ครบถ้วน บริบูรณ์มากขึ้น ตลอดจนสอดคล้องกับกฎหมายลำดับรองที่เกี่ยวข้อง ทำให้ผู้ที่สนใจและสถานประกอบการที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน ได้นำไปปรับใช้ประกอบการดำเนินกิจกรรมที่เกี่ยวกับข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เอกสารฉบับนี้จะเกิดขึ้นมิได้ หากไม่ได้รับการสนับสนุนจาก นายนิยม สองแก้ว อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย ที่ปรึกษาคณะทำงาน และความร่วมแรงร่วมใจจากคณะทำงานของกรมสวัสดิการและคุ้มครองแรงงาน รวมไปถึงหน่วยงานที่เกี่ยวข้องที่ทำให้เกิดเอกสารฉบับนี้ โดยเฉพาะอาจารย์สุกฤษ โกยอัครเดช, อาจารย์สันต์ภพ พรวัฒนะกิจ, อาจารย์มยุรี ชวนชม, อาจารย์ดวงดาว สำนองสุข รวมถึงท่านอื่น ๆ ที่มิได้เอ่ยนามมา ณ ที่นี้

หากท่านมีข้อสังเกต ข้อแลกเปลี่ยนความคิดเห็น ตลอดจนข้อติชมต่าง ๆ หรือหากมีข้อผิดพลาดประการใด สามารถแนะนำได้ที่ pdpasme@smethai.or.th และสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ www.smethai.or.th/pdpasme เพื่อที่จะนำมาใช้ในการปรับปรุงและพัฒนาเอกสารแนวปฏิบัติการคุ้มครองแรงงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ให้เป็นประโยชน์กับทุกฝ่ายต่อไป

กรมสวัสดิการและคุ้มครองแรงงาน

สมาพันธ์เอสเอ็มอีไทย

PDPA Thailand

สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

20 กันยายน 2566

สารบัญ

ความเป็นมา

เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีผลบังคับใช้ทั้งฉบับตั้งแต่วันที่ 1 มิถุนายน 2565 ซึ่งเป็นกฎหมายใหม่ที่มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดยที่เจ้าของข้อมูลส่วนบุคคลนั้นจะเป็นบุคคลธรรมดาที่อาศัยอยู่ในประเทศไทย อันเป็นสาเหตุให้ผู้ใช้แรงงาน พนักงาน และลูกจ้างต่างก็เป็นเจ้าของข้อมูลส่วนบุคคล และมีความจำเป็นที่จะต้องได้รับการคุ้มครองข้อมูลส่วนบุคคลของตนเอง

ขณะเดียวกันกฎหมายฉบับนี้มุ่งเน้นให้นิติบุคคลต้องดำเนินการเพื่อให้เกิดความสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล มิเช่นนั้น จะมีความรับผิดและโทษตามกฎหมาย เป็นเหตุให้สถานประกอบการซึ่งอยู่ภายใต้กฎหมายคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงาน เกิดความวิตกกังวลที่จะต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองแรงงาน และกฎหมายอื่น ๆ ที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

สมาพันธ์เอสเอ็มอีไทยซึ่งเป็นองค์กรเอกชนที่ไม่แสวงหาผลกำไร อันเกิดจากการรวมตัวกันของผู้ประกอบการเอสเอ็มอีไทยจำนวนกว่า 100,000 ราย (www.smethai.or.th) เล็งเห็นถึงความสำคัญในเรื่องดังกล่าว จึงได้ร่วมกับพันธมิตรของสมาพันธ์ฯ ที่มีความเชี่ยวชาญและมีความชำนาญในเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกรมสวัสดิการและคุ้มครองแรงงานจัดตั้งคณะทำงานฯ ขึ้น เพื่อจัดทำแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการขึ้น เพื่อให้เกิดประโยชน์ต่อสถานประกอบการซึ่งอยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

เนื่องจากกฎหมายฉบับนี้มีความจำเป็นที่จะต้องมีกฎหมายระดับรองอีกจำนวนมาก รวมทั้งการบังคับใช้เมื่อเกิดสถานการณ์จริง โดยที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำลังเร่งจัดทำรายละเอียดต่าง ๆ เพิ่มเติม ซึ่งผู้อ่านสามารถติดตามความคืบหน้าและรายละเอียดของกฎหมายระดับรองและการบังคับใช้กฎหมายฉบับนี้ได้ที่ www.pdpc.or.th

คณะทำงานหวังเป็นอย่างยิ่งว่า เอกสารที่ได้จัดทำขึ้นนี้จะเป็นประโยชน์ต่อผู้ใช้แรงงาน พนักงาน และลูกจ้างในสถานประกอบการ ตลอดจนเป็นแนวทางให้สถานประกอบการสามารถนำไปปรับใช้ในการดำเนินกิจกรรมเพื่อให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่อไป และเนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายใหม่ จึงมีความจำเป็นที่จะต้องปรับปรุงและพัฒนาแนวปฏิบัตินี้ให้สมบูรณ์ยิ่งขึ้นในภายภาคหน้า

บทที่ 1 ที่มาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลและความสัมพันธ์กับกฎหมายคุ้มครองแรงงาน

1.1 ที่มาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

วันที่ 25 พฤษภาคม 2561 สหภาพยุโรปได้มีการประกาศการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในชื่อว่า General Data Protection Regulation (GDPR) ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์เพื่อป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบ โดย GDPR บังคับใช้กับทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลของประชาชนที่อาศัยอยู่ในสหภาพยุโรป ไม่ว่าผู้ควบคุมหรือผู้ประมวลผลข้อมูลจะตั้งอยู่ที่ไหน กล่าวคือ บังคับใช้กับผู้ควบคุมและผู้ประมวลผลข้อมูลในสหภาพยุโรป ไม่ว่าการประมวลผลจะทำในสหภาพยุโรปหรือไม่ก็ตาม บังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นในสหภาพยุโรป

นอกจาก GDPR จะมีผลบังคับใช้ภายในประเทศสมาชิกสหภาพยุโรปแล้ว ยังส่งผลถึงผู้ประกอบการในประเทศไทยที่จะต้องดำเนินการติดต่อสื่อสาร หรือรับส่งข้อมูลส่วนบุคคลของประชากรในประเทศที่เป็นสมาชิกของสหภาพยุโรป (Cross-Border Data Transfer Issues) โดยผู้ประกอบการในไทยจำเป็นต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอด้วยในการดำเนินการต่าง ๆ ทางธุรกิจที่มีการประมวลผลข้อมูลส่วนบุคคล

1 ปีต่อมา หลังจากที่สหภาพยุโรปได้มีการประกาศใช้ GDPR ไปแล้วนั้น ประเทศไทยก็ได้มีการประกาศในราชกิจจานุเบกษาในวันที่ 27 พฤษภาคม 2562 เพื่อกำหนดให้หน่วยงานหรือกิจการที่มีการประมวลผล อันได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้อยู่ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562 (2019)) ซึ่งเรียกโดยย่อว่า “PDPA”

โดยกฎหมายฉบับนี้ได้ระบุให้ บุคคล องค์กร หรือหน่วยงานที่เกี่ยวข้องในการดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน ไม่ว่าจะเป็นเอกชนหรือหน่วยงานภาครัฐจะต้องไม่นำเอาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลไปใช้ในกิจกรรมต่าง ๆ โดยปราศจากฐานความยินยอมหรือฐานอื่นที่กฎหมายกำหนด และกฎหมายดังกล่าวได้มีการบังคับใช้อย่างเต็มรูปแบบแล้วเมื่อวันที่ 1 มิถุนายน 2565

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (กฎหมายคุ้มครองข้อมูลส่วนบุคคล) เป็นกฎหมายที่ได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป และบัญญัติขึ้นโดยมีวัตถุประสงค์ในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ในสภาวการณ์ที่การใช้งานข้อมูลส่วนบุคคลกลายเป็นเรื่องที่จำเป็นและมีความสำคัญในทุกภาคส่วน ไม่ว่าจะเป็นหน่วยงานของรัฐหรือองค์กรธุรกิจภาคเอกชน ผลของความจำเป็นดังกล่าวอาจส่งผลต่อเจ้าของข้อมูลส่วนบุคคล เช่น การโทรขายสินค้าหรือการแลกเปลี่ยนข้อมูลเพื่อประโยชน์ทางธุรกิจที่อาจกระทบถึงความเป็นส่วนตัวในชีวิตประจำวันของบุคคล เป็นต้น

บทบัญญัติในกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีลักษณะพิเศษแตกต่างจากกฎหมายฉบับอื่น กล่าวคือ ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่จะมุ่งเน้นสร้างความตระหนักรู้ การทบทวน และกลไกในการพิจารณาเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต่าง ๆ เพื่อให้การกระทำใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวภายใต้หลักการของกฎหมาย

1.2 เจตนารมณ์ของกฎหมายกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นกฎหมายว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคล โดยมีการสร้างมาตรฐานในการรักษาความปลอดภัยและความเป็นส่วนตัวข้อมูลส่วนบุคคล ให้มีการนำไปใช้อย่างตรงตามวัตถุประสงค์ และตรงตามความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้อนุญาตหรือมีฐานที่ชอบด้วยกฎหมาย

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ไม่เพียงแต่เข้ามาเป็นมาตรฐานด้านความปลอดภัยและการใช้ข้อมูล แต่ยังเป็นการส่งเสริมและสนับสนุนให้เกิดการใช้ประโยชน์ของข้อมูลส่วนบุคคลอย่างปลอดภัยและเป็นไปตามมาตรฐานสากล นอกจากนี้ประเทศไทยยังมีนโยบายเศรษฐกิจดิจิทัล (Thailand Digital Economy Policy) เพื่อส่งเสริมและผลักดันให้เกิดเศรษฐกิจดิจิทัล แต่ประเด็นที่เกี่ยวกับความมั่นคงปลอดภัย (Cybersecurity) ของประเทศไทยนั้นยังมีความอ่อนแอ จึงจำเป็นอย่างยิ่งที่จะต้องหันมาให้ความสำคัญในเรื่องนี้

1.3 ความเป็นส่วนตัว (Information Privacy)

ความเป็นส่วนตัว (Information Privacy) หมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น โดยสิทธินี้ใช้ได้อย่างครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล องค์กร และหน่วยงานต่าง ๆ

การละเมิดข้อมูลส่วนบุคคลในสังคมไทยและการฟ้องร้องนั้นเกิดขึ้นมาอย่างยาวนานโดยที่ยังไม่มี พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหากจะฟ้องร้องเรื่องการละเมิดความเป็นส่วนตัวนั้น จะอยู่ในหัวข้อเรื่องของ “ความเป็นส่วนตัว” และต้องฟ้องตามประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยละเมิด

1.4 ทำไมจึงต้องมีกฎหมาย PDPA

(1) การละเมิดข้อมูลส่วนบุคคล เนื่องจากที่ผ่านมามีการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากอันส่งผลให้เกิดความเดือดร้อนหรือส่งผลให้เกิดความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลนั้น

(2) เทคโนโลยีสารสนเทศ ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีสารสนเทศเป็นสาเหตุสำคัญที่ทำให้ การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเกิดปัญหาในการถูกละเมิดได้โดยง่าย และรวดเร็วซึ่งก่อให้เกิดความเสียหายทั้งต่อตัวบุคคลและต่อเศรษฐกิจโดยรวม

(3) กฎหมาย มีการกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

1.5 การป้องกันข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลที่เกี่ยวข้องกับบุคคลอันจะสามารถระบุตัวตนของบุคคลนั้น ๆ ได้ ทั้งทางตรงและทางอ้อม เว้นแต่กรณีข้อมูลของผู้เสียชีวิตจะไม่นับเป็นข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคลจะแบ่งออกเป็น 2 ประเภท ดังนี้

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data)
หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล หรือชื่อเล่น / เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลข	หมายถึง ข้อมูลที่เป็นเรื่องส่วนบุคคลโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและอาจสุ่มเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เป็นข้อมูลส่วนบุคคลอีกประเภทที่ พ.ร.บ.คุ้มครองข้อมูลส่วน

ใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล) / ที่อยู่, อีเมล, เลขโทรศัพท์ / ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน / ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง / ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file / ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต	บุคคลฉบับนี้ให้ความสำคัญและมีบทลงโทษที่รุนแรงในกรณีเกิดการรั่วไหลสู่สาธารณะ ได้แก่ เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสุขภาพ, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ, ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

เหตุที่ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data) เป็นข้อมูลที่มีบทลงโทษที่รุนแรงกว่าข้อมูลส่วนบุคคลทั่วไป (Personal Data) เนื่องจากข้อมูลประเภทนี้เมื่อมีการรั่วไหลสู่สาธารณะแล้ว จะเกิดผลเสียที่ร้ายแรงกับผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้มากกว่าข้อมูลส่วนบุคคลอื่น ๆ และมีผลต่อสิทธิเสรีภาพของบุคคล เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย การไม่ถูกเลือกปฏิบัติ ซึ่งอาจจะก่อให้เกิดการแทรกแซงซึ่งสิทธิเสรีภาพและการเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป ตัวอย่างเช่น ข้อมูลพฤติกรรมทางเพศ เชื้อชาติ ศาสนา ประวัติอาชญากรรม ถ้ารั่วไหลไปแล้ว ข้อมูลเหล่านี้จะนำมาสู่ความเป็นอคติและจะมีผลกระทบต่อชีวิตส่วนบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไปเป็นอย่างมาก

1.6 ขอบเขตการบังคับใช้กฎหมาย PDPA (Law Enforcement)

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) บังคับใช้กับใคร

(1) ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ที่ “อยู่ในราชอาณาจักร” ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นจะกระทำ “ใน” หรือ “นอก” ราชอาณาจักรก็ตาม

(2) ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ที่ “อยู่นอกราชอาณาจักร” แต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในราชอาณาจักร โดยมีการดำเนินกิจกรรม ดังนี้

มีการเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูล (ไม่ว่าจะมีการชำระเงินหรือไม่) ในราชอาณาจักร

มีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

กรณีศึกษา 1: ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อยู่ในประเทศไทย ได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคนที่อยู่ในประเทศไทย หรือการเก็บข้อมูลที่อยู่นอกประเทศ เช่น การสรรหา รับสมัครงานบุคคลสัญชาติอื่น การกรอกข้อมูลนอกประเทศของผู้ควบคุมข้อมูลส่วนบุคคล กรณีนี้บริษัทนั้นจะต้องอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

กรณีศึกษา 2: บริษัทอยู่ต่างประเทศ มีการก่อตั้งอยู่นอกราชอาณาจักรไทย ตัวอย่างเช่น Google, Line, Facebook กรณีนี้จะดำเนินการอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) หากบริษัทนั้นได้มีการนำเสนอการขายสินค้าหรือบริการหรือเฝ้าติดตามพฤติกรรม กับเจ้าของข้อมูลในราชอาณาจักร (ไม่จำกัดสัญชาติ)

ดังนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) จึงมีผลในการบังคับใช้กับบุคคลและหน่วยงานแทบจะทั้งหมด เช่น ผู้ประกอบการ – เจ้าของธุรกิจ หุ้นส่วน คู่ค้า ลูกค้า – ผู้บริโภค พนักงาน – ลูกจ้าง หรือหน่วยงานภาครัฐ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ไม่บังคับใช้กับใคร

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) มาตรา 4 ได้กำหนดไว้ ดังนี้

(1) การประมวลผลข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัวหรือในครอบครัว

(2) การดำเนินการของหน่วยงานรัฐในเรื่องความมั่นคงของรัฐ ความมั่นคงทางการคลัง การรักษาความปลอดภัยของประชาชน การป้องกันปละปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือความมั่นคงปลอดภัยไซเบอร์

(3) การประมวลผลข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมตามจริยธรรมวิชาชีพหรือประโยชน์สาธารณะ

(4) การประมวลผลข้อมูลส่วนบุคคลของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวในการพิจารณาตามหน้าที่และอำนาจของสภาหรือคณะกรรมาธิการดังกล่าว

(5) การพิจารณาพิพากษาคดีของศาล กระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ และการดำเนินกระบวนยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

นอกจากนี้ ได้มีกฎหมายลำดับรองกำหนดให้ในบางกรณีนั้น ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อาจจะไม่ต้องปฏิบัติตาม PDPA ในหมวด 2 เรื่องการคุ้มครองข้อมูลส่วนบุคคลและหมวด 3 เรื่องสิทธิของเจ้าของข้อมูล หากเข้าหลักเกณฑ์ตามที่กฎหมายกำหนดไว้ ซึ่งก็คือ “พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บางส่วนมาใช้บังคับ พ.ศ.2566”

โดยกฎหมายลำดับรองฉบับนี้ ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลทั้งภาครัฐและภาคเอกชน ได้รับยกเว้นในการปฏิบัติตามหมวด 2 และหมวด 3 ในกรณีดังต่อไปนี้

(1) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการทุจริต เช่น ป.ป.ช. ป.ป.ท. หรือหน่วยงานรัฐที่คณะกรรมการประกาศกำหนด

(2) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจาก กรมสรรพากร กรมศุลกากร หรือกรมสรรพสามิต ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีอากรและความร่วมมือระหว่างประเทศเกี่ยวกับภาษี

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้ และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(3) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากองค์กรปกครองส่วนท้องถิ่นที่คณะกรรมการประกาศกำหนด ที่มีกฎหมายให้อำนาจขอข้อมูลส่วนบุคคลเพื่อการจัดเก็บภาษีที่ดินและสิ่งปลูกสร้าง

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(4) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากสำนักเลขาธิการคณะรัฐมนตรีเพื่อดำเนินการตามวัตถุประสงค์หรือภารกิจตามกฎหมายเกี่ยวกับการสถาปนาสมณศักดิ์ การแต่งตั้งหรือถอดถอนข้าราชการ บุคคลหรือคณะบุคคล ซึ่งเป็นพระราชอำนาจของพระมหากษัตริย์ หรือที่ต้องเสนอคณะรัฐมนตรี และการขอพระราชทาน หรือเรียกคืนเครื่องราชอิสริยาภรณ์ ฎีกาซึ่งมีผู้ทูลเกล้าฯถวาย หรือการขอพระราชทานพระมหากรุณาในเรื่องต่าง ๆ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิรู้ว่าหน่วยงานดังกล่าวเก็บข้อมูลใดเกี่ยวกับตนไว้และมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบันได้

(5) กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการร้องขอข้อมูลส่วนบุคคลจากหน่วยงานรัฐที่มีกฎหมายให้อำนาจเพื่อดำเนินการตามวัตถุประสงค์เกี่ยวกับประโยชน์สาธารณะที่สำคัญตามที่คณะกรรมการประกาศกำหนด

(6) กรณีการประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการเนรเทศ การส่งผู้ร้ายข้ามแดน ความร่วมมือระหว่างประเทศเกี่ยวกับกระบวนการยุติธรรมทางอาญา การป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ความร่วมมืออื่นทางศาล หรือกระบวนการยุติธรรมระหว่างประเทศ

(7) การประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐตามพระราชกฤษฎีกานี้ บรรดาที่มีกฎหมายหรือพระราชกฤษฎีกานี้ให้อำนาจในการขอข้อมูลส่วนบุคคลเพื่อดำเนินการตามหน้าที่และอำนาจที่กฎหมายกำหนดไว้ หน่วยงานของรัฐซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลดังกล่าวย่อมได้รับการยกเว้นเช่นเดียวกัน

แม้ว่าผู้ควบคุมข้อมูลส่วนบุคคลตามที่ระบุไว้ในพระราชกฤษฎีกาข้างต้นจะได้รับการยกเว้นการปฏิบัติตาม PDPA ในหมวด 2 และ 3 แต่เขาก็ยังคงมีหน้าที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศของคณะกรรมการ

1.7 ความสัมพันธ์ระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกฎหมายคุ้มครองแรงงาน

หลังจากที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้มีการประกาศใช้อย่างเป็นทางการเต็มรูปแบบแล้วในวันที่ 1 มิถุนายน 2565 กฎหมายฉบับนี้ได้เข้าไปมีบทบาทสำคัญอย่างมากในทุกอุตสาหกรรมที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ในแง่ของการคุ้มครองแรงงาน มีกิจกรรมต่าง ๆ และข้อมูลของพนักงานที่กฎหมายดังกล่าวเข้าไปเกี่ยวข้อง โดยไม่จำกัดเพียงแค่ภาครัฐเท่านั้น แต่ยังรวมไปถึงภาคเอกชนที่มีการประมวลผลข้อมูลของพนักงานภายในองค์กรด้วย ซึ่งกฎหมายสำคัญที่เข้ามาเกี่ยวข้อง คือ กฎหมายคุ้มครองแรงงาน ไม่ว่าจะเป็นกิจกรรมการคัดเลือกพนักงาน การทำสัญญาจ้างแรงงาน การพัฒนาบุคลากร การอนุมัติเลื่อนตำแหน่ง หรือแม้แต่การพ้นสภาพการจ้างของพนักงาน

ตัวอย่างเช่น ในการจัดทำทะเบียนลูกจ้างตามพระราชบัญญัติคุ้มครองแรงงาน มาตรา 15 ได้มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้เก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดการจ้าง จะเห็นได้ชัดว่าการกำหนดระยะเวลาการทำลายข้อมูลดังกล่าวตามกฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดรายละเอียดการทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการดำเนินการลบหรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว โดยเป็นไปตามหลัก “การจัดเก็บข้อมูลอย่างจำกัด (storage limitation)” หรือ กิจกรรมที่เกี่ยวกับการขอลาของพนักงาน กฎหมายคุ้มครองแรงงานได้มีการกำหนดให้นายจ้างมีอำนาจขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่ถ้าเป็นกรณีที่ลาไม่เกิน 3 วันหรือกรณีที่นำไปใช้เพื่อวัตถุประสงค์อื่น นายจ้างมีหน้าที่ต้องขอความยินยอมจากลูกจ้าง เป็นต้น

บทที่ 2 นิยามและบุคคลที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน

2.1 นิยามของข้อมูลส่วนบุคคล

2.1.1 ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล ชื่อเล่นลูกจ้าง หมายเลขโทรศัพท์ลูกจ้าง เลขประจำตัวประชาชนลูกจ้าง เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่พนักงาน เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร รหัสพนักงาน วันเริ่มงาน เงินเดือน ตำแหน่งงาน ข้อมูลภาพถ่ายการอบรมหรือประชุมของพนักงาน เอกสารประกอบการลา ประวัติการศึกษา เป็นต้น

อย่างไรก็ดี ข้อมูลต่อไปนี้ไม่ใช่ข้อมูลส่วนบุคคล เช่น ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล อาทิ ชื่อบริษัท ที่อยู่ของบริษัท เลขทะเบียนนิติบุคคลของบริษัท หมายเลขโทรศัพท์ของที่ทำงาน ที่อยู่อีเมล (email address) ที่ใช้ในการทำงานหรือกลุ่มของบริษัท เช่น info@company.co.th ข้อมูลนิรนาม (Anonymous Data) ข้อมูลผู้ถึงแก่กรรม เป็นต้น

2.1.2 ข้อมูลส่วนบุคคลละเอียดอ่อน (Sensitive Data)

ข้อมูลส่วนบุคคลประเภทนี้อาจเรียกกันในหลายแบบ เช่น ข้อมูลส่วนบุคคลประเภทพิเศษหรือข้อมูลอ่อนไหว โดยข้อมูลประเภทนี้จะเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ข้อมูลประเภทนี้นายจ้างต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อนต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือในกรณีที่นายจ้างมีความจำเป็นต้องดำเนินการตามที่กฎหมายอนุญาต เช่น การเก็บข้อมูลประวัติอาชญากรรมของลูกจ้าง นายจ้างไม่สามารถเก็บได้ เว้นแต่ได้รับความยินยอมหรือมีฐานรองรับตามที่กฎหมายกำหนด หรือ

ในกรณีของการเก็บข้อมูลใบรับรองแพทย์ซึ่งมีข้อมูลสุขภาพ นายจ้างไม่สามารถเก็บได้เว้นแต่ได้รับความยินยอมหรือหรือมีฐานรองรับตามที่กฎหมายกำหนด

2.2 นิยามของการประมวลผลข้อมูล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย (PDPA) ไม่ได้มีนิยามสำหรับคำว่า “การประมวลผลข้อมูล” ไว้ แต่ว่า GDPR ของสหภาพยุโรปได้กำหนดนิยามไว้ ดังนี้

“การประมวลผลข้อมูล หมายถึง การดำเนินการใด ๆ หรือชุดของการดำเนินการที่กระทำกับข้อมูลส่วนบุคคล จะโดยวิธีการแบบอัตโนมัติหรือไม่ก็ตาม เช่น การรวบรวม การบันทึก การจัดการอย่างเป็นระบบ การจัดโครงสร้าง การประยุกต์หรือแก้ไข การกู้คืน การให้คำปรึกษา การใช้ การเปิดเผยด้วยการส่ง การเปิดเผยด้วยการเผยแพร่หรือเข้าถึงได้โดยวิธีอื่นใด การรวมข้อมูล การจำกัด การลบหรือทำลาย”[1]

แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย (PDPA) จะไม่ได้กำหนดนิยามไว้อย่างชัดเจนเหมือนกับ GDPR แต่ก็ได้กำหนดถึงลักษณะของการกระทำเกี่ยวกับข้อมูลส่วนบุคคลในแง่วิธีการ คือ “การเก็บรวบรวม ใช้ หรือเปิดเผย” หรือ “ลบหรือทำลาย” ซึ่งเมื่อพิจารณาแล้วจะเห็นได้ว่าสอดคล้องกับลักษณะ “การประมวลผลข้อมูล” ของ GDPR นั่นเอง

2.3 บุคคลที่เกี่ยวข้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน

2.3.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของข้อมูล (Ownership) หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลนี้จะหมายถึงบุคคลธรรมดาเท่านั้น และไม่รวมถึง “นิติบุคคล” (Juristic Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท สมาคม มูลนิธิ หรือองค์กรอื่นใด อีกทั้งไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมด้วย ทั้งนี้ เจ้าของข้อมูลส่วนบุคคล ได้แก่ บุคคลดังต่อไปนี้

1. เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะ หมายถึง
    - บุคคลที่มีอายุตั้งแต่ 20 ปีบริบูรณ์ขึ้นไป
    - ผู้ที่สมรสตามกฎหมายตั้งแต่อายุ 17 ปีบริบูรณ์ขึ้นไป
    - ผู้ที่สมรสก่อนอายุ 17 ปี โดยศาลอนุญาตให้ทำการสมรส

[1] GDPR Article 4 (2)

- ผู้เยาว์ซึ่งผู้แทนโดยชอบธรรมให้ความยินยอมในการประกอบธุรกิจทางการค้าหรือธุรกิจอื่น หรือในการทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน ในความเกี่ยวพันกับการประกอบธุรกิจ หรือ การจ้างแรงงานข้างต้นให้ผู้เยาว์มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว

ทั้งนี้ ในการให้ความยินยอมใด ๆ เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะสามารถให้ความยินยอมได้ด้วยตนเอง

เจ้าของข้อมูลส่วนบุคคลที่เป็น “ผู้เยาว์” หมายถึง บุคคลที่อายุต่ำกว่า 20 ปีบริบูรณ์ และไม่ใช่ผู้บรรลุนิติภาวะตามข้อ 1 ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

2. เจ้าของข้อมูลส่วนบุคคลที่เป็น “คนเสมือนไร้ความสามารถ” หมายถึง บุคคลที่ศาลสั่งให้เป็นคนเสมือนไร้ความสามารถเนื่องจากมีกายพิการหรือมีจิตฟั่นเฟือนไม่สมประกอบ หรือประพฤติสุรุ่ยสุร่ายเสเพลเป็นอาจิณ หรือติดสุรายาเมา หรือมีเหตุอื่นใดทำนองเดียวกันนั้น จนไม่สามารถจะจัดทำการงานโดยตนเองได้ หรือจัดกิจการไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือครอบครัว ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถนั้นก่อน

3. เจ้าของข้อมูลส่วนบุคคลที่เป็น “คนไร้ความสามารถ” หมายถึง บุคคลที่ศาลสั่งให้เป็นคนไร้ความสามารถ เช่น เป็นบุคคลวิกลจริต ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถนั้นก่อน

2.3.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นผู้ประกอบการที่ทำธุรกิจในนามบุคคลธรรมดา หรือทำในรูปแบบนิติบุคคล และไม่ว่าจะเป็นขนาดเล็กหรือขนาดใหญ่ ประกอบกิจการเป็นบริษัทจำกัด หรือบริษัทมหาชนจำกัด และไม่ได้จำกัดแต่เฉพาะในภาคธุรกิจเท่านั้น หน่วยงานของรัฐก็เช่นกัน หากเขาเหล่านั้นมีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เขาจะมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งหน้าที่ของผู้ควบคุมข้อมูล มีดังนี้

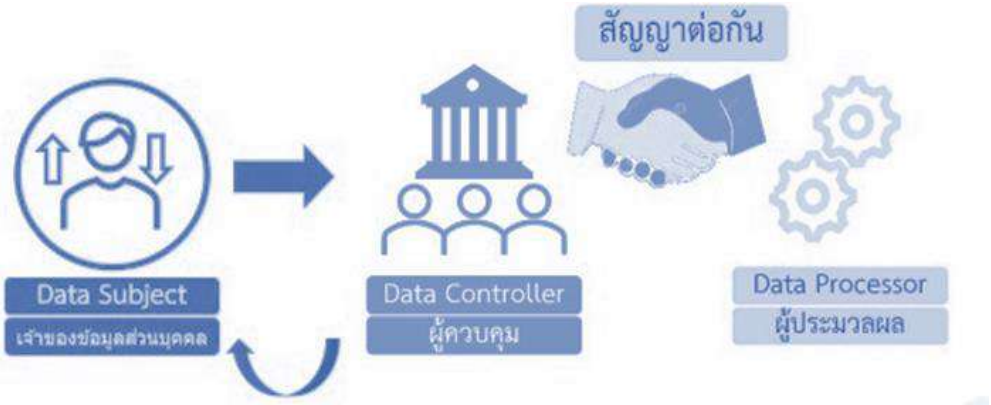
หน้าที่	รายละเอียด
1.เก็บรวบรวม ใช้ เปิดเผย ให้เป็นไปตามกฎหมาย	การเก็บรวบรวม ใช้ เปิดเผย ต้องมีฐานทางกฎหมายรองรับ ดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ และต้องดำเนินการเก็บรวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคลเว้นแต่เข้าข้อยกเว้น ซึ่งเกี่ยวข้องกับหน้าที่ในการจัดเตรียมเอกสารต่าง ๆ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมั่นใจว่า หากยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลเข้าไปเก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอย่างไร ตัวอย่างเช่น นายจ้างมีหน้าที่ต้องจัดเก็บรวบรวมข้อมูลลูกจ้าง ได้แก่ ชื่อ นามสกุล วันที่เริ่มจ้าง อัตราค่าจ้าง เพื่อจัดทำทะเบียนลูกจ้างตามกฎหมายคุ้มครองแรงงาน เป็นต้น
2.เปิดช่องให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมาย	บันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เมื่อผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมระบุเหตุผลในรายการบันทึกรายการตามมาตรา 39 ตัวอย่างเช่น พนักงานของนายจ้างขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคล แต่การเข้าถึงดังกล่าวนั้นไปกระทบสิทธิของบุคคลอื่น กรณีเช่นนี้ นายจ้างมีสิทธิในการปฏิเสธได้ และต้องมีการบันทึกเหตุแห่งการปฏิเสธไว้
3.จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล	เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเป็นไปตามมาตรฐานขั้นต่ำ ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของลูกจ้างว่า ในกิจกรรมนั้น ๆ ฝ่ายใดมีสิทธิในการเข้าถึง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อคกุญแจหรือไม่
4.จัดให้มีมาตรการป้องการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ	ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น มีการโอนข้อมูลส่วนบุคคลให้ผู้ประมวลผล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ถูกต้องตามกฎหมาย

หน้าที่	รายละเอียด
5.จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้	จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ตัวอย่างเช่น ข้อมูลทะเบียนลูกจ้างควรมีการจัดเก็บอย่างน้อย 2 ปี และควรมีการทำลายเมื่อหมดความจำเป็นในการจัดเก็บ หรือในกรณีที่มีข้อพิพาทระหว่างนายจ้างกับลูกจ้าง นายจ้างอาจสามารถเก็บได้ถึง 10 ปี ตามอายุความที่กฎหมายกำหนดไว้
6.แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	ต้องแจ้งเหตุละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับแต่เมื่อทราบเหตุดังกล่าว ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ล่าช้า
7.แต่งตั้งตัวแทนในราชอาณาจักร	หากผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลต้องแต่งตั้งตัวแทนของตนในประเทศไทย โดยต้องแต่งตั้งเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในประเทศไทยและได้รับมอบอำนาจให้กระทำแทนโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูล
8.หน้าที่ในการจัดทำบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities: RoPA)	ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์
9.จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล	การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้

หน้าที่	รายละเอียด
ส่วนบุคคล (Data Processing Agreement: DPA)	มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล
10.แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)	หากเข้าหลักเกณฑ์ที่กฎหมายกำหนดให้ต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ หากองค์กรเป็นผู้ตัดสินใจจะเก็บรวบรวมข้อมูลส่วนบุคคลของใคร ใช้ข้อมูลอะไร มีวัตถุประสงค์อย่างไร ถือว่าเข้าข่ายเป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่ไม่ได้มีหน้าที่แค่จัดทำประกาศความเป็นส่วนตัว

2.3.3 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่ง หรือ ในนามหรือภายใต้คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล



ความสัมพันธ์ 3 ฝ่าย

เมื่อเจ้าของข้อมูลส่วนบุคคลได้มอบความไว้วางใจและให้ข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะต้องมีความรอบคอบในการเก็บรักษาข้อมูล ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลทำข้อมูลรั่วไหล บุคคลคนแรกที่จะต้องรับผิดชอบ คือ ผู้ควบคุมข้อมูลส่วนบุคคล ดังนั้น จึงจะต้องมีการทำสัญญาร่วมกันเพื่อกำหนดมาตรฐานในการดำเนินการภายใต้ PDPA ให้เกิดความรับผิดชอบร่วมกัน และจำเป็นจะต้องสร้างความเข้าใจร่วมกัน ดังนี้

1) พนักงานในหน่วยงาน องค์กร หรือสถาบัน ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) กล่าวคือ พนักงาน และ ลูกจ้าง ทุกระดับ ไม่ว่าจะเป็นเจ้าหน้าที่ ผู้จัดการ หรือผู้บริหาร ที่แม้จะมีอำนาจตัดสินใจก็เป็นเพียงตัวแทน หรือผู้แทนที่กระทำการในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
2) พนักงานในหน่วยงาน องค์กร หรือสถาบัน ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) พนักงานของนิติบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่กระทำตามคำสั่งหรือในนามของนิติบุคคลนั้น พนักงานไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล มีดังนี้

หน้าที่	**รายละเอียด**
1. ประมวลผลข้อมูลส่วนบุคคลภายใต้คำสั่งผู้ควบคุมข้อมูล	ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น นายจ้างมีการจ้างบริษัทภายนอก เพื่อดำเนินการด้านเงินเดือนให้กับลูกจ้าง บริษัทที่รับประมวลดังกล่าวต้องทำตามคำสั่ง หากทำนอกคำสั่งผู้ประมวลผลจะกลายเป็นผู้ควบคุมข้อมูลในกิจกรรมที่ทำนอกคำสั่งนั้น
2.จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของลูกจ้างในองค์กรว่า ในกิจกรรมนั้น ๆ ว่าฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อคกุญแจหรือไม่
3.จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล	จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด
4.ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล	การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมส่วนบุคคลต้องจัดให้มี

	ข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

2.3.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

คุณสมบัติและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) นั้น จะเป็นพนักงาน หรือเป็นผู้รับจ้างของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลก็ได้ และอาจจะเป็นคนเดียวหรือคณะทำงานก็ได้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลส่วนบุคคลและรายละเอียดการประมวลผลภายในองค์กร ได้รับการสนับสนุนที่เพียงพอ ด้านอุปกรณ์ เครื่องมือ งบประมาณ และอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ ได้รับความคุ้มครองจากการถูกเลิกจ้างด้วยเหตุที่ปฏิบัติหน้าที่ตามกฎหมายนี้ และสามารถรายงานถึงผู้บริหารสูงสุดขององค์กรได้โดยตรง

การกำหนดให้แต่ละองค์กรต้องมีเจ้าหน้าที่คุ้มครองส่วนบุคคลหรือไม่นั้น กฎหมาย (มาตรา 41) ได้กำหนดไว้เป็น 3 กรณี ดังนี้

กรณีที่หนึ่ง หน่วยงานรัฐที่จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41 (1)) ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้กำหนดรายชื่อหน่วยงานไว้ เช่น สำนักงานคณะกรรมการข้าราชการพลเรือน กรมบัญชีกลาง กรมการกงสุล กรมการท่องเที่ยว กรมการขนส่งทางบก กรมพัฒนาธุรกิจการค้า กรมการปกครอง กรมการจัดหางาน กรมพัฒนาฝีมือแรงงาน สำนักงานประกันสังคม กรุงเทพมหานคร การทางพิเศษแห่งประเทศไทย ธนาคารกรุงไทย ธนาคารออมสิน มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น[2]

กรณีที่สอง ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) ซึ่งได้มีการวาง

[2] สามารถดูรายชื่อหน่วยงานรัฐทั้งหมดตามประกาศได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf

หลักเกณฑ์ที่สำคัญ กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะครบทั้ง 3 องค์ประกอบ จะต้องมีการแต่งตั้ง DPO โดยองค์ประกอบทั้งสามประการ มีดังนี้[3]

องค์ประกอบประการแรก การดำเนินกิจกรรมในการประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) โดยกิจกรรมหลัก หมายถึง การดำเนินการที่จำเป็นและสำคัญต่อเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล แต่ไม่รวมถึงกิจกรรมเสริมที่เป็นงานสนับสนุนในการดำเนินงานซึ่งไม่ใช่การดำเนินงานที่จำเป็นและสำคัญเพื่อบรรลุวัตถุประสงค์ในการดำเนินงานในกิจการของผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล

ในประกาศฯ ได้ยกตัวอย่างว่า การประมวลผลข้อมูลส่วนบุคคลของลูกค้าเพื่อการให้บริการแก่ลูกค้าและบันทึกการรับบริการของลูกค้าเป็นการดำเนินการที่จำเป็นและสำคัญต่อการให้บริการรับจ้างขนส่งสินค้าหรือการประมวลผลข้อมูลส่วนบุคคลจากกล้องวงจรปิดเป็นการดำเนินการที่จำเป็นและสำคัญต่อการรับจ้างรักษาความปลอดภัย แต่ไม่รวมถึงงานสนับสนุนด้านบุคลากรและเทคโนโลยีสารสนเทศซึ่งเป็นเพียงงานสนับสนุนสำหรับการให้บริการรับจ้างขนส่งสินค้าหรือการรับจ้างรักษาความปลอดภัยให้กับสถานที่ต่าง ๆ

องค์ประกอบประการที่สอง การดำเนินกิจกรรมนั้นมีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ หมายถึง การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลักที่มีการเฝ้าติดตาม (track) เฝ้าสังเกต (monitor) วิเคราะห์ หรือทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคลอย่างเป็นระบบ (profile) และเกิดขึ้นเป็นประจำหรือปกติธุระ (regular)

โดยในกรณีดังต่อไปนี้ จะถือเป็นกรณีที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ

- การประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์ หรือบัตรอื่นใดที่มีลักษณะเดียวกันซึ่งผู้ให้บริการสามารถตรวจสอบรายละเอียดข้อมูลการใช้งานบัตรได้

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการซึ่งเกิดเป็นปกติธุระหรือประจำ ที่มีการตรวจสอบสถานะ ประวัติ คุณสมบัติก่อนเข้าทำสัญญาหรือให้บริการเพื่อประเมินความเสี่ยงด้านต่าง ๆ เช่น การให้คะแนนเครดิต การพิจารณาเบี้ยประกันภัย การป้องกันการฉ้อฉล เป็นต้น

[3] สามารถดูรายละเอียดของประกาศฉบับนี้ได้ที่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาติดตามพฤติกรรม (behavioral advertising)

- การประมวลผลข้อมูลส่วนบุคคลของของลูกค้าหรือผู้รับบริการโดยผู้ให้บริการระบบเครือข่ายคอมพิวเตอร์หรือผู้ประกอบกิจการโทรคมนาคม

- การประมวลผลข้อมูลส่วนบุคคลเพื่อการเฝ้าระวังและรักษาความปลอดภัยตามสถานที่ต่าง ๆ

- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

และองค์ประกอบประการสุดท้าย กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale) โดยจะพิจารณาจากปัจจัย ดังต่อไปนี้

- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง หรือสัดส่วนเจ้าของข้อมูลที่ประมวลผล เมื่อเทียบกับจำนวนเจ้าของข้อมูลทั้งหมดที่อาจเป็นไปได้

- ปริมาณ ประเภท หรือลักษณะของข้อมูลส่วนบุคคลที่ประมวลผล

- ระยะเวลาหรือความคงอยู่ของการประมวลผลเพื่อประโยชน์ในการดำเนินกิจกรรมหลัก

- ขอบเขตการใช้ข้อมูลส่วนบุคคลขององค์กร หรือตามขนาดพื้นที่หรือจำนวนประเทศที่เกี่ยวข้องกับการประมวลผล

โดยในกรณีดังต่อไปนี้ จะถือเป็น กรณีที่มีข้อมูลส่วนบุคคลจำนวนมาก (on a large scale)

- การประมวลผลข้อมูลส่วนบุคคลจำนวนตั้งแต่ 100,000 รายขึ้นไป

- การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม ผ่านโปรแกรมค้นหาหรือสื่อสังคมออนไลน์

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานโดยปกติของบริษัทตามกฎหมายว่าด้วยประกันชีวิตและกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

- การประมวลผลข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้รับใบอนุญาตประกอบธุรกิจโทรคมนาคมแบบที่สามตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม

- กรณีอื่นตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ดังนั้น หากผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายใดที่การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) ที่จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ และมีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

กรณีที่สาม หากกิจกรรมหลักกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลประเภทอ่อนไหว (มาตรา 26) ก็ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย (มาตรา 41 (3))

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีดังนี้

หน้าที่	รายละเอียด
1.ให้คำแนะนำ	ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
2.ตรวจสอบการดำเนินการ	ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
3.ประสานงานและให้ความร่วมมือกับสำนักงาน	ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4.รักษาความลับของข้อมูล	รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

บทที่ 3 หลักการคุ้มครองข้อมูลส่วนบุคคลกับการคุ้มครองแรงงาน

3.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

หลักการคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน มี 7 หลักการ ดังนี้

3.1.1 หลักการถูกกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness Fairness and Transparency)

การประมวลผลข้อมูลส่วนบุคคลจะมีขึ้นได้เฉพาะกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นมีเหตุผลความจำเป็นที่สามารถอ้างอิงฐานการประมวลผลข้อมูลส่วนบุคคลทางกฎหมาย (legal basis) ที่กฎหมายรับรอง โดยจะต้องมีการประกาศและแสดงต่อลูกจ้างทราบถึงเหตุผลความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลอย่างเปิดเผย และง่ายต่อการทำความเข้าใจเพื่อให้ลูกจ้างสามารถตัดสินใจต่อการประมวลผลข้อมูลที่อาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้ (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 23 มาตรา 24)

ตัวอย่างเช่น นายจ้างเก็บข้อมูลทะเบียนลูกจ้างตามกฎหมายคุ้มครองแรงงาน สามารถใช้ฐาน “การปฏิบัติตามกฎหมาย” ตามมาตรา 24 (6) ในการจัดเก็บข้อมูลส่วนบุคคลของลูกจ้างได้ และต้องแจ้งประกาศความเป็นส่วนตัวให้ลูกจ้างทราบถึงวัตถุประสงค์ในการประมวลผลข้อมูลดังกล่าวตามมาตรา 23

3.1.2 หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)

การประมวลผลข้อมูลส่วนบุคคลสามารถกระทำได้อย่างจำกัดเท่าที่จำเป็นภายใต้ขอบเขตวัตถุประสงค์ที่แจ้งไว้กับลูกค้า เพื่อให้การประมวลผลข้อมูลส่วนบุคคลสอดคล้องตามหลักความชอบด้วยกฎหมาย เป็นธรรม และความโปร่งใสอย่างแท้จริง เว้นแต่กรณีที่มีวัตถุประสงค์ใหม่และวัตถุประสงค์นั้นเกี่ยวข้องหรือสอดคล้องกับวัตถุประสงค์เดิม (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 21)

ตัวอย่างเช่น การเก็บข้อมูลสุขภาพของลูกจ้าง เพื่อใช้ในการดำเนินการเป็นเอกสารอ้างอิงประกอบการลาป่วย เมื่อป่วยเกิน 3 วัน ตามกฎหมายคุ้มครองแรงงาน นายจ้างจะนำข้อมูลดังกล่าวไปใช้ในวัตถุประสงค์นอกเหนือจากการใช้เป็นเอกสารประกอบการลาไม่ได้ เว้นแต่ได้รับความยินยอมจากลูกจ้าง

3.1.3 หลักการใช้ข้อมูลอย่างจำกัด (Data Minimization)

การประมวลผล เก็บรวบรวม ใช้ เปิดเผย และระยะเวลาเก็บข้อมูล ควรดำเนินการเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และควรพิจารณาอย่างรอบคอบ (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 22)

ตัวอย่างเช่น การจัดเก็บสำเนาบัตรประชาชน ซึ่งมีข้อมูลศาสนาซึ่งเป็นข้อมูลอ่อนไหวตามมาตรา 26 นายจ้างต้องพิจารณาว่าการเก็บข้อมูลศาสนาดังกล่าว นายจ้างมีความจำเป็นต้องเก็บหรือไม่ เพราะถ้าหากไม่มีความจำเป็นในการเก็บแล้ว ควรมีมาตรการ เช่น การถมดำ หรือ การขีดฆ่าข้อมูลศาสนา เพื่อเป็นการลดภาระและปัญหาที่ตามมาจากการเก็บข้อมูลอ่อนไหว

3.1.4 หลักความถูกต้องของข้อมูล (Data Accuracy)

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) จะต้องดำเนินการเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบ หรือแก้ไขโดยไม่ชักช้า และควรมีการจัดช่องทางการติดต่อที่ง่าย สะดวก รวดเร็ว (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 35)

ตัวอย่างเช่น เมื่อลูกจ้างแจ้งเปลี่ยนแปลงชื่อ นามสกุล ต่อนายจ้าง นายจ้างก็มีหน้าที่ในการแก้ไขชื่อนามสกุลของลูกจ้างเพื่อให้ข้อมูลส่วนบุคคลถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

3.1.5 หลักการจำกัดการจัดเก็บข้อมูล (Storage Limitation)

ข้อมูลส่วนบุคคลจะต้องเก็บในระยะเวลาที่เหมาะสม เพื่อให้เป็นไปวัตถุประสงค์ในการประมวลผลข้อมูล หรือตามกฎหมายอื่น ๆ (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 37 (3))

ตัวอย่างเช่น ในกิจกรรมการจัดทำทะเบียนลูกจ้างตามกฎหมายคุ้มครองแรงงาน ได้มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้จัดเก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดการจ้างแต่ละราย การกำหนดระยะเวลาการทำลายข้อมูลดังกล่าว กฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดเวลาในการจัดเก็บและทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการดำเนินการลบหรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว

3.1.6 หลักความสมบูรณ์และความลับของข้อมูล (Integrity and Confidentiality)

มาตรการที่จะรักษาความปลอดภัยให้ข้อมูลส่วนบุคคลนั้นจะต้องมีความสมบูรณ์ ไม่ผิดเพี้ยนที่จะต้องไม่มีใครแก้ไขข้อมูลโดยไม่มีสิทธิ มีการเก็บข้อมูลส่วนบุคคลอย่างเป็นความลับที่ต้องไม่มีใครเข้าถึงข้อมูลโดยไม่มีสิทธิ และความพร้อมใช้งานที่ต้องไม่มีใครเข้าครอบครองข้อมูลโดยไม่มีสิทธิ (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 37 (1))

ตัวอย่างเช่น กรณีนายจ้างเก็บรักษาสำเนาบัญชีธนาคารของลูกจ้าง ก็ต้องมีมาตรการในการเก็บรักษาไว้ในที่ปลอดภัย โดยไม่ให้พนักงานทุกคนเข้าถึงได้โดยง่าย และจะเข้าถึงได้เฉพาะพนักงานที่เกี่ยวข้องเท่านั้น

3.1.7 หลักความรับผิดชอบ (Accountability)

หลักการนี้เป็นภาพสะท้อนทั้ง 6 หลักที่กล่าวมาข้างต้น นอกจากนี้ หากผู้ควบคุมหรือประมวลผลข้อมูลไม่ปฏิบัติตามหลักการเหล่านี้ จะมีความรับผิดและโทษตามที่กฎหมายกำหนดไว้ (มาตราที่สะท้อนหลักการนี้ เช่น มาตรา 37 (4) มาตรา 81 เป็นต้น)

ตัวอย่างเช่น บริษัทนายจ้างใช้ข้อมูลละเอียดอ่อนของลูกจ้างโดยไม่มีฐานทางกฎหมาย จึงเป็นการฝ่าฝืนตามมาตรา 26 และมาตรา 27 โดยประการที่น่าจะทำให้ลูกจ้างเกิดความเสียหาย ในกรณีนี้ หากการฝ่าฝืนกฎหมายดังกล่าวเกิดจากการสั่งการของกรรมการผู้มีอำนาจดำเนินงานของบริษัท กรรมการผู้นั้นต้องรับโทษทางอาญาด้วยตามมาตรา 81

3.2 ฐานทางกฎหมาย (มาตรา 24)

ในการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการคุ้มครองแรงงาน กฎหมายคุ้มครองข้อมูลส่วนบุคคล มาตรา 24 กำหนดฐานทางกฎหมายไว้ 7 ฐาน ดังต่อไปนี้

3.2.1 ฐานความยินยอม

มาตรา 19 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยการให้ความยินยอมมีหลักเกณฑ์ ดังนี้

1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล
2) การขอความยินยอมต้องทำโดยชัดแจ้ง
3) แจ้งวัตถุประสงค์อย่างชัดเจน
4) ต้องไม่เป็นส่วนหนึ่งของสัญญา
5) เข้าถึงได้ง่าย เข้าใจง่าย
6) การให้ความยินยอมต้องมีความอิสระ
7) ต้องถอดถอนง่ายและจะถอนความยินยอมเมื่อใดก็ได้ โดยบทเฉพาะกาล มาตรา 95 ผู้ควบคุมข้อมูลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม และต้องกำหนดวิธีการยกเลิกความยินยอม ตลอดจนประชาสัมพันธ์ให้เจ้าของข้อมูลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย เช่น ผ่านเว็บไซต์ แต่มีข้อควรระวัง กล่าวคือ ในเรื่องของความสัมพันธ์

ระหว่างนายจ้างและลูกจ้างที่มีลักษณะเป็นความสัมพันธ์ที่ไม่เท่าเทียมกัน อาจเกิดความไม่เป็นอิสระในการให้ความยินยอม

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง
2) ผู้เยาว์อายุ 10 – 20 ปี อาจให้ความยินยอมโดยลำพัง หรือจาก ผู้ใช้อำนาจปกครองผู้เยาว์
3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์
4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

ตัวอย่างเช่น นายจ้างจะเปิดเผยข้อมูลส่วนบุคคลของลูกจ้างเพื่อวัตถุประสงค์ด้านการตลาด นายจ้างจะต้องขอความยินยอมของลูกจ้างก่อน

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของเข้ามูลส่วนบุคคล เว้นแต่

3.2.2 ฐานปฏิบัติตามสัญญา

ฐานสัญญาถือเป็นฐานที่จำเป็นเพื่อการปฏิบัติตามสัญญาและใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา เช่น การขอสินเชื่อเพื่อเปิดบัญชีเงินฝาก การให้สินเชื่อ การทวงถามหนี้สินที่ต้องประมวลข้อมูลการเงิน โดยฐานปฏิบัติตามสัญญา จำเป็นเพื่อปฏิบัติตามสัญญาโดยตรงทั้งก่อนและเข้าทำสัญญาทางการค้าแม้ไม่ได้ระบุเป็นเงื่อนไขในสัญญา เฉพาะข้อมูลส่วนบุคคลทั่วไปของเจ้าของข้อมูลคู่สัญญาเท่านั้น เมื่อเข้าฐานปฏิบัติตามสัญญาก็ไม่ต้องขอความยินยอมเพิ่มเติม และเมื่อไม่ใช่ฐานความยินยอมจึงไม่อาจถอนความยินยอมได้

ตัวอย่างเช่น ในการทำสัญญาจ้างแรงงาน นายจ้างสามารถเก็บรวมรวมชื่อ นามสกุล ที่อยู่ ซึ่งเป็นข้อมูลส่วนบุคคลของลูกจ้างได้โดยไม่จำต้องขอความยินยอมจากลูกจ้าง

3.2.3 ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล

ในฐานนี้มี “ความจำเป็น” ตามกฎหมาย ไม่ใช่ทางเลือกเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล แต่เป็นหน้าที่ตามบทบัญญัติแห่งกฎหมายที่ตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ

ตัวอย่างเช่น พ.ร.บ.คุ้มครองแรงงาน กำหนดให้นายจ้างมีหน้าที่ยื่นภาษีให้กรมสรรพากรตามมาตรา 76[4] นายจ้างจำเป็นต้องประมวลข้อมูลส่วนบุคคลโดยอาศัย ชื่อ นามสกุล บัตร ประจำตัวประชาชน เลขผู้เสีย

[4] ชำระภาษีได้ตามจำนวนที่ลูกจ้างต้องจ่าย

ภาษี หรือนายจ้างต้องจัดทำทะเบียนลูกจ้างตามมาตรา 112 ซึ่งต้องเก็บรวบรวมชื่อ นามสกุล สัญชาติ เพศ วัน เดือนปีเกิด ที่อยู่ เงินเดือน ตำแหน่ง ดังนั้น นายจ้างสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ตามฐานนี้ โดยไม่จำต้องขอความยินยอมจากลูกจ้าง

3.2.4 ฐานผลประโยชน์สาธารณะ

ผู้ประมวลผลข้อมูลตามฐานนี้มักเป็นเจ้าหน้าที่ หรือองค์กรของรัฐที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนหากการประมวลผลข้อมูลนั้นมีความจำเป็นตามอำนาจของรัฐหรือเป็นไปเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยภารกิจดังกล่าวจะต้องมีความชัดเจนและสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

ตัวอย่างเช่น บริษัทนายจ้างให้ลูกจ้างลงชื่อก่อนเข้าสำนักงานเพื่อจะใช้ในการแจ้งเตือนสถานการณ์โรคระบาด

3.2.5 ฐานผลประโยชน์อันชอบธรรมด้วยกฎหมาย

ฐานนี้เป็นกรณีที่จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล และเป็นไปอย่างสมเหตุสมผล เช่น การตรวจสอบอาชญากรรมและการฉ้อโกงอันส่งผลต่อหน่วยงานหรือเป็นการช่วยเหลือเจ้าหน้าที่รัฐตามกฎหมาย โดยมีหลักพิจารณา 3 ข้อ ดังนี้

(1) จะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล

(2) มีความเสี่ยงต่อการกระทบสิทธิเสรีภาพของเจ้าของข้อมูลในระดับต่ำ

(3) มีความชอบธรรม (สำคัญ)

ตัวอย่างเช่น นายจ้างติดตั้งระบบ GPS ในรถขนเงินของนายจ้างที่ลูกจ้างใช้ระหว่างปฏิบัติหน้าที่ เพื่อป้องกันอาชญากรรม นายจ้างย่อมสามารถใช้ฐานนี้ได้ โดยไม่จำต้องขอความยินยอมจากลูกจ้าง

3.2.6 ฐานระงับอันตรายต่อร่างกาย สุขภาพ และชีวิต

ฐานนี้เป็นกรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อปกป้องประโยชน์ที่เกี่ยวข้องกับชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล โดยมาตรานี้จะใช้กรณีเป็นข้อมูลส่วนบุคคลทั่วไป ส่วนกรณีตามมาตรา 26 จะเป็นข้อมูลละเอียดอ่อน (sensitive data) เช่น หมู่เลือด ข้อมูลสุขภาพ

ตัวอย่างเช่น กรณีลูกจ้างหมดสติแล้วนายจ้างนำตัวส่งโรงพยาบาล นายจ้างจึงแจ้งชื่อ นามสกุลของลูกจ้างต่อโรงพยาบาล (กรณีนี้เป็นการเปิดเผยข้อมูลส่วนบุคคลประเภททั่วไป มิใช่ข้อมูลละเอียดอ่อนตามมาตรา 26)

3.2.7 ฐานการจัดทำเอกสารประวัติศาสตร์-วิจัย-สถิติ

ในฐานนี้ไม่มีใน GDPR อย่างไรก็ตาม การใช้ฐานนี้ควรเป็นไปตามมาตรฐานการวิจัยเพื่อการจัดทำเอกสารทางประวัติศาสตร์ หรืองานวิจัย หรืองานสถิติ ซึ่งจะต้องมีการระบุอย่างชัดเจน

3.3. ฐานทางกฎหมาย (มาตรา 26)

ฐานทางกฎหมายตามมาตรานี้จะใช้ในการประมวลผลข้อมูลส่วนบุคคลประเภทละเอียดอ่อนซึ่งมี 6 ฐาน ดังต่อไปนี้

3.3.1. ฐานความยินยอม

มาตรา 19 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยการให้ความยินยอมมีหลักเกณฑ์ ดังนี้

1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล
2) การขอความยินยอมต้องทำโดยชัดแจ้ง
3) แจ้งวัตถุประสงค์อย่างชัดเจน
4) ต้องไม่เป็นส่วนหนึ่งของสัญญา
5) เข้าถึงได้ง่าย เข้าใจง่าย
6) การให้ความยินยอมต้องมีความอิสระ
7) ต้องถอดถอนง่ายและจะถอนความยินยอมเมื่อใดก็ได้ โดยบทเฉพาะกาล มาตรา 95 ผู้ควบคุมข้อมูลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิมและต้องกำหนดวิธีการยกเลิกความยินยอม ตลอดจนประชาสัมพันธ์ให้เจ้าของข้อมูลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย เช่น ผ่านเว็บไซต์ แต่มีข้อควรระวัง กล่าวคือ ในเรื่องของความสัมพันธ์ระหว่างนายจ้างและลูกจ้างที่มีลักษณะเป็นความสัมพันธ์ที่ไม่เท่าเทียมกัน อาจเกิดความไม่เป็นอิสระในการให้ความยินยอม

ตัวอย่างเช่น ในการทำสัญญาจ้าง นายจ้างจะให้ลูกจ้างตรวจสุขภาพในงานที่กฎหมายไม่ได้กำหนดให้ต้องตรวจ นายจ้างจะต้องขอความยินยอมจากลูกจ้างก่อน

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง
2) ผู้เยาว์อายุ 10 – 20 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครองผู้เยาว์
3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์

4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

มาตรา 26 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของเข้ามูลส่วนบุคคล เว้นแต่.....

3.3.2 ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ฐานระงับอันตรายต่อร่างกายสุขภาพและชีวิต กรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อน (sensitive data) เช่น กรุ๊ปเลือด ข้อมูลสุขภาพ เป็นต้น

ตัวอย่างเช่น ลูกจ้างประสบอุบัติเหตุจนหมดสติ นายจ้างจึงเปิดเผยข้อมูลสุขภาพของลูกจ้างแก่โรงพยาบาลเพื่อใช้ในการปกป้องอันตรายที่เกิดขึ้นของลูกจ้าง

3.3.3 ฐานการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร โดยต้องไม่เปิดเผยไปสู่บุคคลภายนอก

ตัวอย่างเช่น สหภาพแรงงานใช้ข้อมูลการเป็นสมาชิกสหภาพแรงงานของลูกจ้างเพื่อกิจกรรมภายในองค์กรสหภาพแรงงานเอง

3.3.4 ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างเช่น ลูกจ้างเปิดเผยต่อสาธารณะว่าตนมีประวัติสุขภาพหรือพฤติกรรมทางเพศแบบใด

3.3.5 จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ตัวอย่างเช่น นายจ้างเก็บข้อมูลสุขภาพของลูกจ้างเพื่อให้การต่อศาลในคดีที่ลูกจ้างฟ้องเรียกค่าเสียหายในปัญหาสุขภาพอันเกิดจากการทำงาน

3.3.6 จำเป็นต้องปฏิบัติตามกฎหมาย

ฐานนี้มีความเกี่ยวข้องกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์การประเมิน ความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการใช้บริการด้านสังคมสงเคราะห์ (ข) ประโยชน์สาธารณะด้านสาธารณสุข (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์หรือสถิติ หรือ (จ) ประโยชน์สาธารณะอื่นที่สำคัญ

ตัวอย่างเช่น นายจ้างเก็บบันทึกข้อมูลสุขภาพของลูกจ้างที่ทำงานเกี่ยวกับสารเคมีอันตรายไว้เพื่อให้เจ้าหน้าที่ตรวจสอบ[5]

3.4 สิทธิของเจ้าของข้อมูล

สิทธิของเจ้าของข้อมูลส่วนบุคคล มี 9 ข้อ ดังนี้

3.4.1 สิทธิในการถอนความยินยอม

ตามมาตรา 19 วรรค 5 กำหนดไว้ดังนี้

1) การถอนความยินยอมจะต้องถอนเมื่อใดก็ได้
2) ต้องถอนได้โดยวิธีที่ง่ายเหมือนเมื่อตอนให้ความยินยอม
3) การถอนต้องไม่มีผลย้อนหลังและไม่ส่งผลต่อการประมวลที่ยินยอมไปแล้ว
4) ถ้าข้อมูลติดฐานอื่น เช่น ฐานสัญญา ฐานปฏิบัติตามกฎหมาย จะไม่สามารถถอนความยินยอมได้

นายจ้างต้องแจ้งลูกจ้างหากลูกจ้างได้ให้ความยินยอมให้นายจ้างเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล (ไม่ว่าจะเป็นความยินยอมที่ลูกจ้างให้ไว้ก่อนวันที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับหรือหลังจากนั้น) ลูกจ้างมีสิทธิที่จะถอนความยินยอมเมื่อใดก็ได้ ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลอยู่กับนายจ้าง เว้นแต่มีข้อจำกัดสิทธินั้นโดยกฎหมายหรือมีสัญญาที่ให้ประโยชน์อยู่

ทั้งนี้ นายจ้างควรแจ้งรายละเอียดว่า การถอนความยินยอมอาจส่งผลกระทบต่อการใช้สิทธิประโยชน์ใด ๆ หรือไม่ได้รับข้อมูลข่าวสารอันเป็นประโยชน์

ตัวอย่างเช่น ลูกจ้างแจ้งถอนความยินยอมในการนำข้อมูลส่วนบุคคลไปใช้ด้านการตลาดของนายจ้าง นายจ้างต้องปฏิบัติตามและแจ้งลูกจ้างว่าหากถอนความยินยอมดังกล่าว ลูกจ้างจะไม่ได้สิทธิประโยชน์ด้านการตลาดนั้น

3.4.2 สิทธิขอเข้าถึงข้อมูลส่วนบุคคล

สิทธิขอเข้าถึงข้อมูลส่วนบุคคลตามมาตรา 30 มีดังนี้

1) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูล ที่เกี่ยวกับตน หรือ ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ไม่ได้ให้ความยินยอม
2) ต้องทำตามคำขอโดยไม่ชักช้าไม่เกินระยะเวลา 30 วันนับแต่วันที่ได้รับคำขอ
3) สามารถปฏิเสธได้หากเป็นไปตามกฎหมายด้วยคำสั่งศาล

[5] กฎกระทรวงกำหนดมาตรฐานการตรวจสุขภาพลูกจ้างซึ่งทำงานเกี่ยวกับปัจจัยเสี่ยง พ.ศ. 2563

4) หากสามารถปฏิเสธได้ ต้องบันทึกการปฏิเสธคำขอพร้อมเหตุผล มาตรา 39
5) ลูกจ้างมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน และขอให้นายจ้างทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้ รวมถึงขอให้นายจ้างเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของนายจ้าง ทั้งนี้ นายจ้างอาจปฏิเสธคำขอหากการเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น หรือนายจ้างต้องปฏิบัติตามกฎหมาย หรือคำสั่งศาลที่ห้ามเปิดเผยข้อมูลส่วนบุคคลนั้น

ตัวอย่างเช่น ลูกจ้างขอเข้าถึงประวัติการทำงานของตนที่นายจ้างบันทึกไว้ หรือขอเข้าถึงข้อมูลส่วนบุคคลที่นายจ้างได้มาจากฐานกฎหมายอื่นที่ไม่ใช่ฐานความยินยอม นายจ้างต้องทำตามคำขอ เว้นแต่จะมีสิทธิปฏิเสธตามกฎหมายหรือคำสั่งศาล และการใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลของลูกจ้างจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

3.4.3 สิทธิในการได้รับแจ้ง

ลูกจ้างมีสิทธิในการที่จะได้ทราบถึงรายละเอียดเกี่ยวกับการใช้ข้อมูลส่วนบุคคลโดยนายจ้าง ซึ่งนายจ้างต้องทำการแจ้งก่อนหรือขณะที่การประมวลผลข้อมูลส่วนบุคคลนั้นจะเริ่มมีขึ้น เพื่อลูกจ้างสามารถตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลอันอาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้ ในแง่นี้ สิทธิดังกล่าวจึงเรียกร้องให้นายจ้างจัดให้มีการแจ้งด้วยการสื่อสารที่ชัดเจนและเข้าใจง่ายตามมาตรา 23 ดังนี้

1) วัตถุประสงค์ในการเก็บและฐานทางกฎหมาย
2) กรณีต้องใช้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือตามสัญญา
3) การเก็บข้อมูลนั้นเป็นการเก็บอะไร เก็บนานเท่าใด
4) จะมีการเปิดเผยข้อมูลให้หน่วยงานใดบ้าง
5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล สถานที่ติดต่อ วิธีการติดต่อ รายละเอียดของผู้เป็น DPO
6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างเช่น ก่อนหรือขณะเข้าทำสัญญาจ้างแรงงาน นายจ้างจะต้องแจ้งรายละเอียดประกาศความเป็นส่วนตัวแก่ลูกจ้างทราบว่า นายจ้างจะประมวลผลข้อมูลของลูกจ้างเพื่อวัตถุประสงค์ใด ใช้ฐานกฎหมายใดใช้ข้อมูลส่วนบุคคลประเภทใด และกรณีเป็นการใช้ฐานปฏิบัติตามกฎหมายหรือสัญญานายจ้างก็ต้องแจ้งรายละเอียดเพิ่มเติม จะเก็บข้อมูลส่วนบุคคลไว้นานเท่าใด ข้อมูลส่วนบุคคลดังกล่าวอาจจะถูกเปิดเผยแก่องค์กรหรือหน่วยงานใด รายละเอียดการติดต่อผู้ควบคุมข้อมูล และสิทธิต่าง ๆ ของลูกจ้างในฐานะเจ้าของข้อมูลส่วนบุคคล

3.4.4 สิทธิในการโอนย้ายข้อมูล

เจ้าของข้อมูลมีสิทธิขอรับข้อมูลจากผู้ควบคุมข้อมูล ถ้าข้อมูลอยู่ในรูปแบบที่สามารถอ่านได้และใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลได้ด้วยวิธีการอัตโนมัติ ตามมาตรา 31 สามารถทำได้ ดังนี้

1) ขอให้ส่งข้อมูลไปยังผู้ควบคุมอื่น
2) ขอรับข้อมูลที่ส่งหรือโอนไปให้ผู้ควบคุมข้อมูลอื่นแต่จะใช้ได้เฉพาะฐานความยินยอมและฐานสัญญา แต่จะใช้ไม่ได้กับฐานปฏิบัติหน้าที่ตามกฎหมายหรือการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะและหากเป็นการกระทบกระเทือนสิทธิเสรีภาพผู้อื่น มีสิทธิปฏิเสธคำขอและต้องบันทึกเหตุผลไว้ในรายการตามมาตรา 39

ลูกจ้างมีสิทธิขอรับข้อมูลส่วนบุคคลของตนจากนายจ้าง ในกรณีที่นายจ้างได้จัดทำข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบให้สามารถอ่านหรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิขอให้นายจ้างส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ และมีสิทธิขอรับข้อมูลส่วนบุคคลที่นายจ้างส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่ไม่สามารถดำเนินการได้เพราะเหตุผลทางเทคนิค

ทั้งนี้ ข้อมูลส่วนบุคคลของลูกจ้างข้างต้น ต้องเป็นข้อมูลส่วนบุคคลที่ลูกจ้างได้ให้ความยินยอมแก่นายจ้างในการเก็บรวบรวม ใช้ และ/หรือเปิดเผย หรือเป็นข้อมูลส่วนบุคคลที่นายจ้างจำเป็นต้องเก็บรวบรวม ใช้ และ/หรือเปิดเผยเพื่อให้ลูกจ้างสามารถใช้ผลิตภัณฑ์และ/หรือบริการของนายจ้างได้ตามความประสงค์ซึ่งลูกจ้างเป็นคู่สัญญาอยู่กับนายจ้าง หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนใช้ผลิตภัณฑ์และ/หรือบริการ หรือเป็นข้อมูลส่วนบุคคลอื่นตามที่ผู้มีอำนาจตามกฎหมายกำหนด

ตัวอย่างเช่น ลูกจ้างขอใช้สิทธิโอนย้ายข้อมูลในทะเบียนลูกจ้างจากนายจ้างคนเดิมให้แก่นายจ้างคนใหม่ นายจ้างคนเดิมปฏิเสธการใช้สิทธิดังกล่าวได้ เนื่องจากการทำทะเบียนลูกจ้างเป็นไปตามฐานการปฏิบัติตามกฎหมาย มิใช่ฐานความยินยอมหรือสัญญา

3.4.5 สิทธิคัดค้านการให้ใช้ข้อมูล

ลูกจ้างมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลในเวลาใดก็ได้ หากการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำขึ้นเพื่อการดำเนินงานที่จำเป็นภายใต้ประโยชน์โดยชอบด้วยกฎหมายของนายจ้าง หรือของบุคคลหรือนิติบุคคลอื่น โดยไม่เกินขอบเขตที่สามารถคาดหมายได้อย่างสมเหตุสมผล หรือเพื่อดำเนินการตามภารกิจเพื่อสาธารณประโยชน์ หากยื่นคัดค้านและนายจ้างจะยังคงดำเนินการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปเฉพาะที่สามารถแสดงเหตุผลตามกฎหมาย

ได้ว่ามีความสำคัญยิ่งกว่าสิทธิขั้นพื้นฐาน หรือเป็นไปเพื่อการยืนยันสิทธิตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการต่อสู้ในการฟ้องร้องตามกฎหมาย ตามแต่ละกรณี

ลูกจ้างซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เกี่ยวกับตนเมื่อใดก็ได้ตามมาตรา 32 ซึ่งแบ่งได้เป็น 3 กรณี

กรณีที่ 1 ข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยใช้ฐานประโยชน์สาธารณะ (Public Interest) อันเป็นเพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลตามมาตรา 24 (4) หรือฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 24 (5) แต่ผู้ควบคุมข้อมูลสามารถปฏิเสธคำคัดค้านได้ถ้าตนมีเหตุอันชอบด้วยกฎหมายมากกว่า หรือตนมีเหตุเกี่ยวกับการก่อ ใช้ ปฏิบัติ ยกขึ้นต่อสู้สิทธิเรียกร้อง

กรณีที่ 2 ข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

กรณีที่ 3 ข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อการศึกษาวิจัย แต่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธได้หากจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

ตัวอย่างเช่น นายจ้างแจ้งข่าวสารด้านการตลาดที่ไม่เกี่ยวข้องกับสัญญาจ้างงาน ลูกจ้างสามารถใช้สิทธิในการคัดค้านได้

3.4.6 สิทธิขอให้ลบข้อมูล

สิทธิขอให้ลบข้อมูลและสิทธิที่จะถูกลืมตามมาตรา 33 เจ้าของข้อมูลมีสิทธิขอให้ลบ ทำลาย หรือ ทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ลูกจ้างมีสิทธิขอลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หากเชื่อว่าข้อมูลส่วนบุคคลของท่านถูกเก็บรวบรวม ใช้ และ/หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายที่เกี่ยวข้อง หรือเห็นว่านายจ้างหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ที่เกี่ยวข้องในประกาศความเป็นส่วนตัวฉบับนี้ หรือเมื่อได้ใช้สิทธิขอถอนความยินยอมหรือใช้สิทธิขอคัดค้านตามที่แจ้งไว้ข้างต้นแล้ว เว้นแต่เป็นกรณีที่ต้องปฏิบัติตามกฎหมาย หรือใช้สิทธิเรียกร้องตามกฎหมายที่เกี่ยวข้องในการเก็บรักษาข้อมูลดังกล่าว

ตัวอย่างเช่น นายจ้างยังบันทึกเบอร์มือถือเก่าอันเป็นข้อมูลส่วนบุคคลของลูกจ้างไว้ เมื่อลูกจ้างไม่ได้ใช้เบอร์ดังกล่าวแล้วก็สามารถใช้สิทธิขอให้นายจ้างลบเบอร์มือถือเก่านั้นได้

3.4.7 สิทธิขอให้ระงับใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิขอให้ระงับใช้ข้อมูลได้ตามมาตรา 34 ในกรณีเจ้าของข้อมูลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำให้ข้อมูลเป็นปัจจุบันและผู้ควบคุมอยู่ระหว่างการตรวจสอบ

ตัวอย่างเช่น ลูกจ้างกังวลว่านายจ้างจะส่งจดหมายไปตามที่อยู่เก่า ลูกจ้างมีสิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคลชั่วคราวในกรณีที่นายจ้างอยู่ระหว่างตรวจสอบตามคำร้องขอใช้สิทธิขอแก้ไขข้อมูลส่วนบุคคลของลูกจ้าง หรือกรณีอื่นใดที่นายจ้างหมดความจำเป็นและต้องลบหรือทำลายข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง แต่ลูกจ้างขอให้นายจ้างระงับการใช้แทน

3.4.8 สิทธิในการแก้ไขข้อมูล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการแก้ไขข้อมูลให้ถูกต้อง โดยปกตินายจ้างต้องดำเนินการประมวลผลข้อมูลที่ทันสมัยและถูกต้องอยู่เสมอ ทั้งนี้ ในบางกรณีอาจไม่สามารถรับรู้หรือทราบถึงข้อมูล ที่ถูกต้องในกรณีนี้ลูกจ้างสามารถยื่นคำขอใช้สิทธิแก้ไขข้อมูลให้ถูกต้อง ซึ่งรวมถึงการขอให้ลบข้อมูลเดิมและเพิ่มเติมข้อมูลใหม่ เพื่อให้การประมวลผลเป็นการใช้ข้อมูลที่ถูกต้องสมบูรณ์ และเป็นปัจจุบัน โดยไม่ก่อให้เกิดความเข้าใจผิด และเกิดประโยชน์แก่ลูกจ้างในการที่จะได้รับบริการที่เหมาะสม ทั้งยังช่วยลดความเสี่ยงในการสร้างความเข้าใจผิดต่อผู้อื่นในกรณีที่ข้อมูลที่ผิดเกิดการรั่วไหล ในการนี้เจ้าของข้อมูลนอกจากยื่นคำขอใช้สิทธิแล้ว จะต้องแสดงให้เห็นชัดถึงข้อมูลที่ถูกต้อง เพื่อให้ผู้ควบคุมดำเนินการแก้ไข

ตัวอย่างเช่น ลูกจ้างเปลี่ยนเบอร์มือถือ ลูกจ้างสามารถใช้สิทธิให้นายจ้างแก้ไขจากเบอร์เดิมเป็นเบอร์ปัจจุบันได้

3.4.9 สิทธิในการร้องเรียน

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องเรียน ผู้ควบคุมข้อมูล และ ผู้ประมวลข้อมูลลูกจ้างหรือผู้รับจ้างตามมาตรา 73

ตัวอย่างเช่น ลูกจ้างเห็นว่านายจ้างไม่ตอบสนองการใช้สิทธิการเข้าถึงและขอสำเนาข้อมูลของตนภายในระยะเวลา 30 วันนับแต่วันที่ได้รับคำขอ ลูกจ้างจึงใช้สิทธิร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3.5 โทษและความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

บทลงโทษความรับผิดตามกฎหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) มีดังนี้

โทษอาญา

1) ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) โดยมิชอบหรือนอกเหนือวัตถุประสงค์ ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไปยังต่างประเทศ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย มีโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

2) ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) โดยมิชอบหรือนอกเหนือวัตถุประสงค์ ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไปยังต่างประเทศ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุกไม่เกิน 1 ปีปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

3) ล่วงรู้ข้อมูลเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้แล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

4) กรรมการหรือผู้จัดการหรือบุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคล หากมีการสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจำเป็นเหตุให้นิติบุคคลกระทำความผิดต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย

มีข้อควรระวัง มาตรา 81 กำหนดให้ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุ บุคคลนั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย

โทษทางปกครอง

กระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามกฎที่กำหนดไว้ เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ, ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูล โทษปรับทางปกครองสูงสุด ไม่เกิน 5,000,000 บาท

ความรับผิดทางแพ่ง

กฎหมายได้กำหนดความความรับผิดแพ่งในการกระทำต่อข้อมูลส่วนบุคคลไว้ ดังนี้

- การกระทำที่ฝ่าฝืนข้อห้ามตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ไม่ว่าจะจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม อันเป็นเหตุให้เกิดความเสียหายแก่เจ้าของข้อมูล (ความรับผิดเด็ดขาด)
- ต้องชดใช้ค่าสินไหมทดแทน และมีค่าเสียหายเชิงลงโทษไม่เกิน 2 เท่า

3.6 สิ่งที่นายจ้างต้องเตรียมตัว

3.6.1 การสร้างความรับรู้ขององค์กร

การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะต้องอาศัยการบริหารจัดการแบบบนลงล่าง (top-down) ซึ่งเป็นการสื่อสารจากผู้บริหารไปยังบุคลากรในองค์กร ขณะเดียวกัน จำเป็นอย่างยิ่งที่องค์กรจะต้องสร้างความรู้ความเข้าใจให้กับบุคลากรระดับปฏิบัติการในการปฏิบัติตามกฎหมายจะต้องอาศัยความมีส่วนร่วมจากทุกหน่วยในองค์กร หากหน่วยหนึ่งหน่วยใดในองค์ไม่มีความตระหนัก ไม่ให้ความร่วมมือ หรือเห็นว่าการปฏิบัติตามกฎหมายนี้เป็นภาระ การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่แม้เกิดขึ้นก็อาจมีช่องว่างและในท้ายที่สุดย่อมส่งผลกระทบต่อองค์กรในภาพรวม

3.6.2 วิเคราะห์การทำงาน และค้นหากิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นในองค์กร

กิจกรรมนี้เป็นกิจกรรมหนึ่งที่มีความสำคัญ แต่ละส่วนงานจะต้องพยายามแสดงกระบวนการทำงานวิธีการเส้นทางการใช้งานข้อมูลออกมาให้ชัดเจนและละเอียดที่สุดเท่าที่จะสามารถกระทำได้ โดยอาจอาศัยการทำแบบสอบถาม และการสัมภาษณ์พูดคุยกับฝ่ายงาน เพื่อจัดทำผังการใช้ข้อมูลขององค์กร (data mapping หรือ data flow) เพื่อใช้วิเคราะห์การไหลเวียนของข้อมูลส่วนบุคคลในแต่ละกิจกรรมตั้งแต่กระบวนการการเก็บรวบรวม ใช้ เก็บรักษา เปิดเผย และทำลายข้อมูลส่วนบุคคล เพื่อให้ทราบถึงความเสี่ยงและจะช่วยให้นายจ้างสามารถเห็นภาพของจุดบกพร่องและแก้ไขจุดบกพร่องที่เกี่ยวกับข้อมูลส่วนบุคคลในอนาคต

ในส่วนของแบบสอบถาม จะมุ่งเน้นการสร้างกระบวนการทบทวนการใช้งานข้อมูลในองค์กร (data life cycle) ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผย จัดเก็บ และขั้นตอนการลบหรือทำลายข้อมูลส่วนบุคคล โดยในแบบสอบถามองค์กรอาจพิจารณารายการที่กฎหมายกำหนดในเรื่องบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (มาตรา 39) ไม่ว่าจะเป็นการรักษาความปลอดภัยข้อมูล การกำหนดสิทธิการเข้าถึงข้อมูล

(access control) ระยะเวลาการลบทำลายข้อมูล ความจำเป็นของข้อมูล วิธีการในการเปิดเผยส่งต่อข้อมูล การประเมินความเสี่ยงและผลกระทบเกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

3.6.3. วิเคราะห์ช่องว่างทางปฏิบัติไม่สอดคล้องตามเงื่อนไขที่กฎหมายกำหนด (Gap analysis) และการจัดแนวทางในการรักษาความปลอดภัยของข้อมูลที่เหมาะสม

ในขั้นตอนนี้เป็นขั้นตอนที่องค์กรจะมุ่งทำการวิเคราะห์ถึงรายการที่กฎหมายกำหนดให้องค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการหรือมีการจัดการตามหลักการกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญโดยประเด็นที่เป็นโจทย์สำคัญในการพิจารณาช่องว่างการปฏิบัติตามกฎหมายจะเป็นการพิจารณากับประเด็นดังนี้ ในกรณีที่กฎหมายกำหนดให้มีการตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) องค์กรมีการจัดตั้งและมีการดำเนินการตามหน้าที่ที่กฎหมายกำหนดหรือไม่

1) องค์กรมีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หรือไม่
2) องค์กรมีประกาศความเป็นส่วนตัวหรือไม่ (privacy notice) หรือไม่
3) องค์กรได้จัดให้มีแผนการทำงานที่รองรับการพิจารณา ตรวจสอบ และปรับปรุงบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคลที่อาจมีขึ้นในอนาคต เช่น จัดทำผังการใช้ข้อมูลขององค์กร (data mapping หรือ data flow) อย่างไร
4) องค์กรมีการจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (RoPA) แล้วหรือไม่
5) องค์กรมีแนวทางในการจัดการเกี่ยวความยินยอม และการขอความยินยอม (consent request and consent management) หรือไม่
6) องค์กรมีแนวทางจัดการเกี่ยวกับการโอนย้าย ส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สามที่ชัดเจนหรือไม่
7) องค์กรจัดให้มีการลบทำลายข้อมูล หรือมีนโยบายที่เกี่ยวข้องในการจัดการข้อมูลเมื่อสิ้นสุดความจำเป็นหรือไม่
8) องค์กรจัดให้มีช่องทางในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject's Right Request) หรือไม่
9) กรณีที่องค์กรมีการประมวลผลข้อมูลส่วนบุคคลร่วมกับบุคคลที่สาม โดยเฉพาะอย่างยิ่งกรณีที่เป็นการใช้งานผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรได้จัดให้มีข้อตกลงสัญญา หรือมาตรการคัดเลือกบุคคลที่สามหรือไม่
10) องค์กรมีแนวทางในการเก็บรักษาข้อมูล และมาตรการรักษาความปลอดภัยที่เพียงพอเหมาะสมหรือไม่

11) องค์กรได้จัดให้มีระบบรองรับการทำงานที่เกี่ยวข้องกรณีเกิดเหตุละเมิดรั่วไหลต่อข้อมูลส่วนบุคคลแล้วหรือไม่

3.6.4 การจัดแนวทางในการรักษาความปลอดภัยของข้อมูลที่เหมาะสม

เพื่อให้องค์กรพิจารณาตามเห็นสมควร โดยองค์กรจะพิจารณาเลือกใช้มาตรการมากน้อยเพียงใดนั้น โดยหลักมักขึ้นอยู่กับชั้นการจัดกลุ่มชั้นความลับของข้อมูล (data classification) ความเสี่ยง รวมทั้งความสามารถในด้านงบประมาณขององค์กรสำหรับมาตรการรักษาความปลอดภัยข้อมูลที่องค์กรจะนำมาปรับใช้ อาจพิจารณาแบ่งออกเป็นมาตรการรักษาความปลอดภัยพื้นฐานทั่วไป เช่น การจัดการสิทธิการเข้าถึง การกำหนดนโยบายการใช้งานอุปกรณ์ส่วนตัว ตลอดจนมาตรการทางเทคนิค อาทิ การจัดการชั้นความลับ การเข้ารหัสข้อมูล การแฝงข้อมูล นอกจากนี้ มาตรการรักษาความปลอดภัยยังรวมไปถึงระบบที่เกี่ยวข้องกับการตรวจสอบติดตาม และการจัดการกรณีเกิดเห็นละเมิดรั่วไหลของข้อมูลส่วนบุคคล (data breach)

ในกรณีที่องค์กรไม่สามารถจัดให้มีระบบรักษาความปลอดภัยที่เหมาะสม ไม่ว่าด้วยเหตุผลข้อจำกัดด้านงบประมาณ หรือเหตุผลด้านสัญญาที่องค์กรได้มีการลงทุนระบบที่มีอยู่เดิมไปก่อนหน้า องค์กรควรพิจารณาความจำเป็นในการใช้งานข้อมูลส่วนบุคคลอย่างรอบคอบ โดยอาจยกเลิกกิจกรรมประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นในบางลักษณะ หากองค์กรยังเห็นว่ากิจกรรมประมวลผลดังกล่าวจำเป็นต้องดำเนินต่อไป องค์กรอาจควรจัดให้มีแผนในการเตรียมความพร้อมด้านงบประมาณ หรือแผนการจัดหาผู้ให้บริการที่เหมาะสม และในระหว่างการดำเนินการดังกล่าว องค์กรจะคำนึงถึงการประมวลผลข้อมูลด้วยความระมัดระวังและอาศัยการบริหารจัดการปฏิบัติงานของบุคลากรเพื่อปิดช่องว่าง หรือลดความเสี่ยงที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรแทน

3.6.5 การสร้างองค์ความรู้และความเข้าใจให้กับบุคลากรในองค์กรและการติดตามผลการปฏิบัติงาน

ส่งเสริมให้บุคลากรขององค์กรในระดับปฏิบัติการเกิดความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนแนวทางหรือวิธีการปฏิบัติงานที่เปลี่ยนแปลงไปอันเนื่องมาจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งควรมีการตรวจสอบหรือทำให้แน่ใจว่าบุคลากรในองค์กรมีความตระหนักรู้และเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอที่จะปฏิบัติตามขั้นตอน ข้อกฎหมาย หรือนโยบายคุ้มครองข้อมูลส่วนบุคคลที่องค์กรกำหนดได้อย่างเหมาะสม สำหรับวัตถุประสงค์สำคัญของการเตรียมการเรื่องนี้คือ การทำให้การคุ้มครองข้อมูลส่วนบุคคลเป็นวัฒนธรรมองค์กรและเป็นส่วนหนึ่งของแนวทางการทำงานขององค์กร

การติดตามผลการปฏิบัติตามกฎหมาย (monitoring compliance results) โดยภายหลังองค์กรได้จัดการองค์กร และเตรียมความพร้อมในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วเสร็จ จำเป็นอย่างยิ่งที่องค์กรจะต้องจัดให้มีแนวทางในการติดตามการทำงานเป็นระยะ และเป็นประจำต่อเนื่อง ตั้งแต่ในกระบวนการเก็บบันทึก กระบวนการรักษา ความปลอดภัย ไปจนถึงการลบทำลายข้อมูล เพื่อวัตถุประสงค์ดังนี้

1) เพื่อตรวจสอบผลการปฏิบัติตามกฎหมายให้มีความถูกต้องครบถ้วนอยู่เสมอ
2) เพื่อทบทวนแนวทางการทำงานขององค์กรให้สอดคล้องตามกฎหมายในกรณีที่องค์กรมีกิจกรรมประมวลผลข้อมูลส่วนบุคคลที่เพิ่มขึ้นหรือเปลี่ยนแปลงจากที่มีอยู่เดิม
3) เพื่อเป็นแนวทางป้องกันเหตุอันอาจเกิดได้ในอนาคต

บทที่ 4 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับพนักงาน

หลังจากที่กฎหมายกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้มีการประกาศใช้อย่างเป็นทางการเต็มรูปแบบแล้ว ในวันที่ 1 มิถุนายน พ.ศ. 2565 กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เข้าไปมีบทบาทสำคัญอย่างมากในทุกอุตสาหกรรมที่มีการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ในแง่ของการคุ้มครองแรงงาน มีกิจกรรมต่าง ๆ และข้อมูลของพนักงานที่กฎหมายดังกล่าวเข้าไปเกี่ยวข้อง โดยไม่จำกัดเพียงแค่ภาครัฐเท่านั้น แต่ยังรวมไปถึงภาคเอกชนที่มีการประมวลผลข้อมูลของพนักงานภายในองค์กรด้วย โดยกฎหมายที่สำคัญที่เข้ามาเกี่ยวข้อง คือ กฎหมายคุ้มครองแรงงาน ไม่ว่าจะเป็นกิจกรรมการคัดเลือกพนักงาน การทำสัญญาจ้างแรงงาน การพัฒนาบุคลากร การอนุมัติเลื่อนตำแหน่ง หรือแม้แต่การพ้นสภาพการจ้างของพนักงาน กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เข้าไปมีความเกี่ยวพันทุกกระบวนการ

ตัวอย่างเช่น ในการจัดทำทะเบียนลูกจ้างตาม พ.ร.บ.คุ้มครองแรงงาน มาตรา 115 ได้มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้จัดเก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดการจ้าง จะเห็นได้ชัดว่า การกำหนดระยะเวลาการทำลายข้อมูลดังกล่าวตามกฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดรายละเอียดการทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการดำเนินการลบ หรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว โดยเป็นไปตามหลัก การจัดเก็บข้อมูลอย่างจำกัด (storage limitation) หรือแม้แต่การขอลาของพนักงาน กฎหมายคุ้มครองแรงงานได้มีการกำหนดให้นายจ้างมีอำนาจขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่ถ้าเป็นกรณีที่ลาไม่เกิน 3 วันหรือกรณีที่นำไปใช้เพื่อวัตถุประสงค์อื่น นายจ้างมีหน้าที่ต้องขอความยินยอมจากลูกจ้าง เป็นต้น

เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีการประกาศใช้แล้ว จะมีเรื่องการขอใช้สิทธิของลูกจ้างที่เพิ่มมากขึ้น สิทธิของเจ้าของข้อมูลในส่วนของงานฝ่ายทรัพยากรบุคคล (Human Resources: HR) นั้นจะมีอยู่หลายกรณี เช่น สิทธิขอเข้าถึงทะเบียนเอกสาร การขอสำเนาใบรับรองเงินเดือนหรือใบรับรองการทำงานเพื่อนำไปกู้เงิน เป็นต้น เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) มีผลบังคับใช้แล้ว สิทธิของพนักงานในองค์กรก็จะมีมากขึ้น ดังนั้น บุคลากรในส่วนงาน HR จำเป็นจะต้องเข้าในสิทธิของพนักงานที่มีเพิ่มขึ้น และเพื่อเป็นการป้องกันเหตุต่าง ๆ ที่อาจจะเกิดขึ้นได้จากการประกาศใช้กฎหมาย บุคลากรในฝ่าย HR ควรเก็บข้อมูลส่วนบุคคลของพนักงานให้อยู่ในประเภทและปริมาณเท่าที่จำเป็นต่อการใช้งานตรงตามวัตถุประสงค์ ซึ่งหมายถึงภาระ/ความรับผิดชอบในการจัดการที่น้อยลงตามไปด้วย

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เป็นการแนะนำแนวทางที่ควรปฏิบัติให้กับนายจ้างหรือองค์กร เพื่อดำเนินการให้เป็นไปตามและสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมถึงกฎหมายคุ้มครองแรงงาน โดยกิจกรรมที่เกี่ยวข้องกับการคุ้มครองแรงงานนั้น มีดังนี้

4.1 กิจกรรมการประกาศรับสมัครและคัดเลือกพนักงาน

การสรรหาและคัดเลือกคนเข้าองค์กร (Recruitment and Selection) เป็นขั้นตอนที่มีความสำคัญ เนื่องจากเป็นขั้นตอนแรกที่มีการจัดเก็บข้อมูลส่วนบุคคลของลูกจ้าง ในบางองค์กรโดยเฉพาะองค์กรขนาดใหญ่จะมีแผนกสรรหาบุคลากรที่แยกออกจากแผนกอื่นโดยเฉพาะ แต่ในบางองค์กรนั้นพนักงานอาจจำเป็นที่จะต้องทำงานในหลายหน้าที่

ในการดำเนินการเกี่ยวกับการสรรหาและคัดเลือกพนักงานสามารถแยกช่องทางการรับสมัครหรือช่องทางการสรรหาออกได้เป็น 8 ช่องทาง ดังนี้

1. กรณีผู้สมัครกรอกใบสมัคร ณ สถานที่ทำงาน วิธีการนี้ฝ่าย HR เก็บข้อมูลจากผู้สมัครโดยตรง
2. กรณีผู้สมัครกรอกใบสมัครผ่าน Application Form หรือ Google Form หรือผ่านทางระบบแบบฟอร์มอื่นๆ วิธีการนี้ ฝ่าย HR เก็บข้อมูลจากผู้สมัครโดยตรง
3. กรณีผู้สมัครส่ง CV หรือ Resume มาทาง E-mail วิธีการนี้ฝ่าย HR เก็บข้อมูลจากผู้สมัครโดยตรง
4. กรณีการคัดเลือกพนักงานจากเว็บไซต์จัดหางาน (Job Search) โดยแบ่งได้ 2 ฝ่าย ดังนี้
    1) ฝ่ายนายจ้างจัดซื้อโฆษณา ซื้อสิทธิในการขอเข้าดูข้อมูลผู้สมัคร
    2) ฝ่าย Job Seeker ในข้อนี้บุคคลที่สนใจหางานจะมาโพสต์ข้อมูลไว้และเป็นผู้เข้าดูข้อมูลเอง
5. กรณีใช้บริษัทอื่นในการจัดหาพนักงานที่มีความเหมาะสม
6. กรณีได้รับการแนะนำผู้สมัครงานมาจากบุคคลอื่น
7. กรณีการแนะนำเพื่อนหรือคนรู้จักให้เข้ามาทำงาน (ในส่วนนี้ไม่ว่าผู้แนะนำจะได้ค่าตอบแทนหรือไม่ก็ตาม)
8. กรณีได้รับข้อมูลของผู้สมัครงานมาจากบริษัทในเครือ

4.1.1 สิ่งที่นายจ้างควรพิจารณาเพิ่มเติม

ข้อควรพิจารณาเกี่ยวกับข้อมูลส่วนบุคคล โดยสามารถใช้คำถามดังต่อไปนี้ เพื่อสอบถามถึงความจำเป็นในการเก็บข้อมูลส่วนบุคคล ดังนี้

1) ข้อมูลส่วนบุคคลของผู้สมัคร นายจ้างต้องการข้อมูลส่วนบุคคลมากน้อยเพียงใด
2) ข้อมูลส่วนบุคคลที่ได้มาจากแหล่งต่าง ๆ นายจ้างต้องบริหารจัดการอย่างไร
3) นายจ้างจะเก็บข้อมูลส่วนบุคคลไว้นานเท่าใด

4) นายจ้างจะทำลายข้อมูลส่วนบุคคลอย่างไร เมื่อหมดความจำเป็น

4.1.2 หน้าที่นายจ้างในการแจ้งต่อผู้สมัคร

เมื่อผู้สมัครได้รับการตอบรับการสมัครงาน จะมีการจัดเก็บข้อมูลส่วนบุคคลของพนักงาน รวมถึงข้อมูลอ่อนไหวที่อาจเข้ามาเกี่ยวข้อง เช่น การเก็บข้อมูลสุขภาพ การเก็บข้อมูลศาสนา นอกจากนายจ้างมีหน้าที่ในการต้องแจ้งข้อมูลเมื่อขั้นตอนการประกาศโฆษณาและในขั้นตอนการกรอกใบสมัครเมื่อผ่านการคัดเลือกนั้น นายจ้างที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งประกาศความเป็นส่วนตัวให้ผู้สมัครงานทราบอีกครั้ง แต่จะมีความแตกต่างในเรื่องของข้อมูลที่มีการจัดเก็บ และวัตถุประสงค์ในการจัดเก็บ รวมถึงรายละเอียดในการแจ้งที่แตกต่างออกไปจากขั้นตอนที่มีการส่งตอนที่มีการโฆษณารับสมัครงาน สิทธิในการได้รับแจ้ง เจ้าของข้อมูลส่วนบุคคลต้องได้รับการแจ้งให้ทราบก่อนหรือขณะเก็บข้อมูลตามมาตรา 23 ดังนี้

1) วัตถุประสงค์ในการเก็บและฐานทางกฎหมาย
2) กรณีต้องใช้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือตามสัญญา
3) การเก็บขอมูลนั้นเป็นการเก็บอะไร เก็บนานเท่าใด
4) จะมีการเปิดเผยข้อมูลให้หน่วยงานใดบ้าง
5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล สถานที่ติดต่อ วิธีการติดต่อ รายละเอียดของผู้เป็น DPO
6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

4.2 กิจกรรมการทำสัญญา (Employee Contract)

หลังจากที่ได้รับการคัดเลือกเป็นพนักงานแล้ว ก็จะเข้าสู่ขั้นตอนการทำสัญญาจ้างงาน สัญญาที่เกี่ยวข้องกับการจ้างแรงงานมีหลากหลายรูปแบบ ไม่ใช่เพียงแค่สัญญาจ้างแรงงานเพียงเท่านั้นแต่ยังมีสัญญาการจ้างรูปแบบอื่น ๆ ซึ่งแตกต่างจากสัญญาจ้างแรงงานทั่วไป ตัวอย่างสัญญาที่เกี่ยวข้องกับการทำงาน มีดังต่อไปนี้

4.2.1 สัญญาจ้างแรงงาน

สัญญานี้ทำขึ้นระหว่างฝ่ายนายจ้างและฝ่ายพนักงาน มีลักษณะที่เป็นสัญญาต่างตอบแทนซึ่งนายจ้างมีอำนาจบังคับบัญชาและลูกจ้างได้รับค่าจ้างตอบแทน นอกจากนี้ สัญญาจ้างแรงงานสามารถเกิดขึ้นได้ด้วยการตกลงกันด้วยวาจา อีกทั้งยังมีข้อกำหนดในเรื่องค่าตอบแทน สวัสดิการ และสิทธิประโยชน์ต่าง ๆ ตามที่กฎหมายกำหนดไว้

4.2.2 สัญญารับจ้างทำของ

ในสัญญาจ้างทำของนั้นมักเกิดขึ้นในการทำงานในรูปแบบของการจ้างผู้มีอาชีพอิสระให้ทำงานให้ (freelance) หรือแบบการจ้างชั่วคราวหรือรับเหมาค่าแรง (Outsource) โดยในส่วนนี้อาจจะไม่ได้มาจากขั้นตอนว่าจ้างการสรรหา แต่อาจจะเป็นการตกลงกัน มีการประมูล หรือมีการว่าจ้างกันเป็นรายกรณี โดยสัญญาประเภทนี้จะไม่คำนึงในเรื่องระยะเวลาการทำงานแต่จะเน้นที่ผลลัพธ์ของผลงานที่ผู้ว่าจ้างต้องการ แต่ในสัญญาจะมีการแจ้งวัตถุประสงค์ในการทำกิจกรรมเพื่อให้ได้ผลงานออกมาตามที่ผู้ว่าจ้างต้องการ เช่น แผนกขนส่งมีคำสั่งซื้อ (order) เยอะเกินไป แต่ระบบการขนส่งขององค์กรมีไม่เพียงพอ จึงดำเนินการจ้างแบบ Outsource เข้ามาดำเนินงานเพื่อให้งานเกิดความคล่องตัวและสำเร็จตามต้องการ เป็นต้น

4.2.3 สัญญาค้ำประกัน

ในความหมายตามบริบทนี้ การทำสัญญาค้ำประกัน มี 2 รูปแบบ คือ ค้ำประกันการทำงาน หรือค้ำประกันค่าความเสียหายจากการทำงาน ซึ่งหากเป็นสัญญาค้ำประกันตามกฎหมายแรงงาน กฎหมายมิได้หมายความว่าการค้ำประกันจะสามารถทำได้ทุกตำแหน่ง การค้ำประกันจะทำได้เฉพาะในตำแหน่งที่มีหน้าที่รับผิดชอบทางการเงินโดยตรงหรือผู้ดูแลทรัพย์สินเท่านั้น

4.2.4 สัญญาระหว่างนายจ้าง กับ บริษัทจัดหาแรงงาน

ในบางองค์กรจะมีการใช้การจ้างงานแบบชั่วคราว (Outsource) เป็นสัญญาการบริการระหว่างผู้ค้ากับหน่วยธุรกิจ (Business to Business: B2B) และใช้กันอย่างแพร่หลายโดยเฉพาะธุรกิจอุตสาหกรรมขนาดใหญ่ เช่น อุตสาหกรรมการก่อสร้าง โรงงานอุตสาหกรรม และแม้กระทั่งแรงงานในสำนักงาน เป็นต้น

สัญญาในรูปแบบนี้ควรมีการตั้งประเด็นคำถามเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ดังต่อไปนี้

- การทำสัญญาระหว่างผู้ให้บริการและผู้ว่าจ้าง มีกิจกรรมใดที่เกี่ยวข้องกับการเก็บรวบรวมใช้เปิดเผย ข้อมูลส่วนบุคคลหรือไม่ เพียงใด
- ผู้ว่าจ้างที่ใช้แรงงานที่ส่งมาจากผู้รับเหมา มีการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ ผู้ว่าจ้างต้องตรวจสอบว่าผู้ที่ส่งผู้ใช้แรงงานนั้นมีการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างไร ผู้ใดจะเป็นคนเก็บข้อมูลส่วนบุคคลเหล่านั้น จะมีมาตรการเช่นใด

4.2.5 สัญญาส่งไปฝึกงานหรือทำงานต่างประเทศ

องค์กรที่มีสำนักงานเครือข่ายหรือมีสาขาอยู่ในหลาย ๆ ประเทศ หรือบริษัทที่จะต้องส่งพนักงานไปเรียนรู้กระบวนการทำงานและเทคนิคต่าง ๆ ของบริษัทแม่ หรือบริษัทในเครือนั้น สามารถทำเป็นสัญญาฝึกงานหรือสัญญาส่งตัวไปทำงาน/ฝึกงานต่างประเทศได้

สัญญารูปแบบนี้มีข้อควรระวังใน 2 มาตรา คือ มาตรา 28 และมาตรา 29 โดยหลักการคือ การส่งข้อมูลส่วนบุคคลไปยังต่างประเทศหรือนอกราชอาณาจักรนั้น ประเทศปลายทางนั้น ๆ ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่ต่ำกว่าของประเทศไทย หรือมีความใกล้เคียงกับของประเทศไทย

4.2.6 สัญญาจ้างนักเรียน นักศึกษาในการทำงานแบบชั่วคราว (Part time)

ในสัญญาการจ้างนักเรียน หรือ นักศึกษามาทำงาน Part time นั้น เป็นการทำงานหลังเลิกเรียน และไม่ได้เป็นลูกจ้างทำงานประจำในเวลางาน

การทำงาน Part time หมายถึง การทำงานนอกเวลาเรียน ซึ่งรวมถึงการทำงานในวันเสาร์–อาทิตย์หรือบางครั้งในวันหยุดด้วย จึงจะต้องมีระเบียบข้อบังคับหรือข้อกำหนดที่เข้มงวดว่า นักเรียนหรือนักศึกษาที่จะทำงานให้นายจ้างนั้น ทั้งนอกเวลาและในวันหยุด สามารถทำงานได้ไม่เกินวันละกี่ชั่วโมง หรือเมื่อทำงานในวันธรรมดาของช่วงปิดเทอมจะสามารถทำได้ไม่เกินกี่ชั่วโมง โดยข้อควรระวังนั้น ผู้ว่าจ้างควรตรวจสอบอายุของนักเรียนนักศึกษาเพื่อไม่ให้เกิดความผิดพลาดทางข้อกฎหมายหากผู้ถูกว่าจ้างเป็นผู้เยาว์

4.2.7 ข้อตกลงการรับนักศึกษาเข้าฝึกงาน (MOU ระหว่างนายจ้างกับสถาบันการศึกษา)

ปัจจุบันสถาบันการศึกษาต่าง ๆ มีการทำสัญญา MOU กับองค์กรนายจ้างหรือหน่วยงานเพื่อส่งตัวนักศึกษามาฝึกงาน โดยระบุให้มีการเซ็นสัญญาช่วงที่ต้องการฝึกงานตามหลักสูตรของรายวิชานั้น ๆ

ในกรณีนี้จะเป็นทางสถาบันการศึกษาจะเป็นผู้เซ็นสัญญาร่วมกับนายจ้าง แต่ตัวผู้ฝึกงานซึ่งเป็นนักเรียน นักศึกษา จะไม่ได้อยู่ในสถานะลูกจ้าง อย่างไรก็ตาม ทางองค์กรหรือฝ่ายทรัพยากรบุคคล จะต้องมีการเก็บข้อมูลส่วนบุคคล ประวัตินักเรียนนักศึกษา เช่น ข้อมูลสถาบัน ปีที่เข้าร่วมงาน แผนกที่ทำงาน ช่วงเวลาในการทำงาน ซึ่งการเก็บข้อมูลนักเรียนนักศึกษาถือเป็นขั้นตอนที่ควรต้องระมัดระวัง และมีความสำคัญเทียบเท่ากับการเก็บรวบรวมประวัติของพนักงาน โดยเฉพาะข้อมูลส่วนบุคคลประเภทอ่อนไหวนั้นควรเก็บเท่าที่จำเป็น และหากนายจ้างจะต้องเก็บไฟล์สแกนลายนิ้วมือ กลุ่มเลือด หรือการสแกนใบหน้าของนักเรียนนักศึกษา ทางฝ่ายทรัพยากรบุคคลต้องมีมาตรการและขั้นตอนเหมือนพนักงาน และนอกเหนือจากนั้นเนื่องจากผู้เยาว์จะต้องให้ความยินยอมและความสมัครใจด้วยตนเอง ก็ต้องเพิ่มเติมการให้ความยินยอมเป็นการเฉพาะสำหรับผู้เยาว์

4.2.8 สัญญาจ้างงานผู้พิการ[6]

สำหรับสัญญาประเภทนี้ ในกรณีที่ทางนายจ้างจ้างงานผู้พิการ ซึ่งเป็นการจ้างงานบุคคลผู้พิการตามกฎหมายว่าด้วยคุณภาพชีวิตคนพิการ[7] (พนักงานผู้พิการ 1 คน ต่อพนักงาน 100 คน) ปัจจุบันการทำสัญญาการจ้างงานสามารถทำได้เพราะเป็นฐานของกฎหมาย หากในการเก็บรวบรวม ใช้ หรือเปิดเผย จัดเก็บ การลบ การทำลาย จะเป็นไปในขั้นตอนเทียบเท่าการจ้างพนักงาน หากแต่เพิ่มการให้คำยินยอมสำหรับผู้พิการโดยเฉพาะ

4.2.9 เอกสารที่ในประกอบในขั้นตอนการทำสัญญาจ้างแรงงาน

เอกสารที่ในการประกอบการทำสัญญานั้น ประกอบไปด้วยข้อมูลส่วนบุคคล ซึ่งมีทั้งข้อมูลส่วนบุคคลอ่อนไหว และข้อมูลส่วนบุคคลทั่วไป โดยทั่วไปแล้ว ในกิจกรรมการทำสัญญาการจ้างงานประกอบไปด้วยเอกสารดังต่อไปนี้

1) หน้าสมุดบัญชีธนาคาร จากขั้นตอนการคัดเลือกและสรรหาที่ผ่านมาแล้วนั้น นายจ้างควรพิจารณาว่าเอกสารใดจำเป็นที่ต้องใช้แนบสำหรับสัญญาจ้างงาน หรือเอกสารใดที่ไม่จำเป็น เช่น จำเป็นหรือไม่ที่ต้องขอเอกสารหน้าบัญชีธนาคารตั้งแต่วันแรกที่พนักงานเข้ามาสมัครงานแต่จะเป็นสำหรับผู้ที่ผ่านการสัมภาษณ์งานและเซ็นสัญญาแล้วเท่านั้น

2) สำเนาบัตรประชาชน การทำสัญญาจ้างมีวัตถุประสงค์เพื่อรับคนเข้าทำงาน โดยส่วนมากจะมีการเก็บข้อมูลส่วนบุคคลทั่วไป รวมไปถึงเลขที่บัตรประจำตัวชาชน และ/หรือ สำเนาบัตรประชาชน ซึ่งหากยังจำเป็นในการที่จะรวบรวม นายจ้างควรมีมาตรการให้มีการเซ็นหรือขีดกำกับแจ้งวัตถุประสงค์ของเจ้าของข้อมูลก่อน

3) การตรวจสุขภาพ การตรวจสอบประวัติอาชญากรรม หากนายจ้างต้องการเก็บข้อมูลส่วนบุคคลอ่อนไหวบางรายการ จะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่น การขอตรวจสุขภาพ การขอตรวจประวัติอาชญากรรม การเก็บลายนิ้วมือจากการสแกน ซึ่งกระบวนการเหล่านี้จะต้องดำเนินการอย่างเป็นขั้นตอนและแจ้งวัตถุประสงค์ต่อเจ้าของข้อมูลให้ชัดเจน หรืออาจต้องมีการขอความยินยอมอื่นๆในบางกร ณี เช่น การใช้ GPS ติดตามตัวก็ถือว่าเป็นอีกหนึ่งรายการซึ่งไม่ใช่ข้อมูลส่วนบุคคลอ่อนไหว แต่การใช้ GPS

[6] การว่าจ้างเด็ก นักเรียน นักศึกษา ผู้พิการ จะต้องมีการขอความยินยอมโดยเฉพาะ

[7] พระราชบัญญัติส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ พ.ศ. 2550

ติดตามอาจจะเป็นละเมิดข้อมูลส่วนบุคคลได้ แต่หากจีพีเอสนั้นนำใช้งานกับเครื่องมือหรืออุปกรณ์อื่นๆ เช่น รถของนายจ้าง หรือรถของส่วนกลางที่ขับขี่ออกไป ในกรณีนี้ถือว่าเป็นมาตรการของนายจ้างสำหรับพนักงานผู้ทำหน้าที่ แต่หากรถติด GPS แล้วให้นำไปใช้งานวันหยุดเสาร์-อาทิตย์ก็จะสามารถตรวจสอบที่อยู่ได้ แบบนี้จะเป็นการเข้าไปละเมิดสิทธิส่วนบุคคลมากเกินไป

4.2.10 เอกสารที่นายจ้างต้องจัดทำเมื่อมีการทำสัญญาจ้างกับพนักงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. ประกาศความความเป็นสำหรับพนักงาน
2. หนังสือขอความยินยอม
3. บันทึกรายการประมวลผลข้อมูลส่วนบุคคล โดยมีรายละเอียด ดังนี้

1. ประกาศความเป็นส่วนตัว (Privacy Notice) หรือ การแจ้งสิทธิของเจ้าของข้อมูล ตามมาตรา เพื่อใช้แจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลจากเจ้าของข้อมูลส่วนบุคคล โดยต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อน หรือ ขณะ ที่มีการเก็บข้อมูลครั้งแรกตามมาตรา 23 การแจ้งสิทธิสำหรับผู้สมัคร ประกอบด้วย

1) วัตถุประสงค์
2) ความจำเป็นต้องให้ข้อมูล
3) ระยะเวลาการจัดเก็บ
4) ประเภทของข้อมูลอาจจะต้องมีการเปิดเผย
5) ข้อมูลตัวแทนของผู้ควบคุมข้อมูล
6) สิทธิตามกฎหมาย

1.1 กรณีผู้สมัครงาน กรณีที่มีการใช้บริษัทจัดหางาน เช่น JobsDB, JobBKK เป็นต้น อาจมีการแจ้งโดยเพิ่ม link หรือ QR code เพื่อให้ผู้สมัครงานสามารถอ่านรายละเอียดในการเก็บข้อมูลได้

1.2 กรณีการเก็บข้อมูลพนักงาน โดยเมื่อพนักงานผ่านการสัมภาษณ์แล้ว นายจ้างจะมีการเก็บข้อมูลพนักงานเพิ่มเติม โดยอาจแจ้งแนบไปกับสัญญาจ้างงาน หรืออาจใช้รูปแบบ QR Code เพื่อให้การเข้าถึงเอกสารนั้นง่าย

2 หนังสือขอความยินยอม (Consent Form)

(กรณีไม่ได้รับยกเว้นตามมาตรา 24 และมาตรา 26)

มาตรา 24 (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน ตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

การขอคำยินยอม ต้องระบุวัตถุประสงค์ชัดเจน เข้าใจง่าย ไม่คลุมเครือ และทำให้ผู้ให้คำยินยอมให้คำยินยอมโดยสมัครใจ ปราศจากข้อสงสัย

ตัวอย่างแบบฟอร์ม การขอความยินยอมใช้ข้อมูลส่วนบุคคล

เพื่อประโยชน์ในการคุ้มครองแรงงานภายใต้สัญญาจ้างแรงงาน และการรักษาความปลอดภัยภายในสถานที่ทำงาน บริษัทจำเป็นต้องเก็บ รวบรวม ใช้ และประมวลผลข้อมูลส่วนบุคคลอ่อนไหวของพนักงานได้แก่ ประวัติสุขภาพ ประวัติการรักษาพยาบาล ประวัติอาชญากรรม(ถ้าจำเป็น) และลายนิ้วมือหรือแบบจำลองใบหน้า เพื่อจุดประสงค์ที่ระบุไว้ ทั้งนี้บริษัทรับประกันการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวอย่างเหมาะสมและรับประกันว่าการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวนี้จะดำเนินการตามเงื่อนไขนโยบายการประมวลผลข้อมูลส่วนบุคคลสำหรับพนักงานตามที่บริษัทได้ประกาศไว้

ข้าพเจ้า.....รหัสพนักงาน.....

☐ ยินยอมให้บริษัทเก็บรวบรวมใช้และรวมถึงเปิดเผย ข้อมูลสุขภาพ ประวัติการรักษาพยาบาลของข้าพเจ้าตามวัตถุประสงค์ที่ระบุไว้ในการคุ้มครองและจัดสวัสดิการให้แก่ข้าพเจ้า

☐ ยินยอมให้บริษัทเก็บรวบรวมใช้ ข้อมูลประวัติอาชญากรรมของข้าพเจ้า ตามวัตถุประสงค์ที่ระบุไว้เนื่องจากตำแหน่งงานของข้าพเจ้าจำเป็นต้องได้รับการตรวจสอบ

☐ ยินยอมให้บริษัทเก็บรวบรวมใช้ ลายนิ้วมือหรือแบบจำลองใบหน้าของข้าพเจ้า เพื่อบันทึกการเข้าออกงานและเพื่อความปลอดภัยในพื้นที่สำนักงานของบริษัท

ลงชื่อ.....พนักงาน

วันที่.....

3 บันทึกรายการกิจกรรม (Record of Processing Activities: RoPA) ตามมาตรา 39

การทำบันทึกรายการกิจกรรมนี้เป็นไปตามข้อกำหนดใน PDPA และเป็นหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล โดยต้องมีการบันทึกในรายละเอียด เพื่อเป็นหลักฐาน และในกรณีต้องมีการตรวจสอบเพื่อบันทึกการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ข้อมูลที่การเก็บรวบรวม, วัตถุประสงค์ในการเก็บ, ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล, ระยะเวลาในการเก็บรักษา, สิทธิเจ้าของข้อมูล, การปฏิเสธการใช้สิทธิ, คำอธิบาย

เกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และเพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตรวจสอบได้

4.2.11 หน้าที่ในการจัดทำทะเบียนลูกจ้าง[8]

การจัดทำทะเบียนลูกจ้างตามพระราชบัญญัติคุ้มครองแรงงานจะต้องมีเงื่อนไข ดังนี้

- นายจ้างที่มีลูกจ้างตั้งแต่ 10 คนขึ้นไป
- จัดทำภายใน 15 วันนับแต่วันที่ลูกจ้างเข้าทำงาน
- เก็บไว้ ณ สถานประกอบการ
- เก็บไว้ไม่น้อยกว่า 2 ปี นับแต่วันสิ้นสุดการจ้างลูกจ้างแต่ละราย (มาตรา 115)
- ฝ่าฝืน ปรับ 20,000 บาท (มาตรา 146)

รายการเก็บข้อมูลเพื่อจัดทำทะเบียนลูกจ้าง ประกอบด้วย

1) ชื่อ - นามสกุล
2) เพศ
3) สัญชาติ
4) วันเดือนปีเกิด/อายุ
5) ที่อยู่ปัจจุบัน
6) วันที่เริ่มจ้าง
7) ตำแหน่งหรืองานในหน้าที่
8) อัตราค่าจ้าง/ประโยชน์ตอบแทนอื่นๆ
9) วันสิ้นสุดของการจ้าง

[8] ข้อกำหนดในกฎหมายแรงงาน ในเรื่องการจัดทำทะเบียนลูกจ้าง เป็นหลักการที่สามารถนำไปใช้ในเรื่องการจัดเก็บข้อมูลและเอกสารส่วนบุคคล ก่อนเข้าสู่ขั้นตอนการลบหรือทำลาย

4.3 กิจกรรมการใช้ข้อมูลของพนักงานร่วมกันในหลายบริษัท

4.3.1 ใช้ข้อมูลพนักงานร่วมกันในเครือบริษัทที่อยู่ในประเทศไทย

บริษัทในเครือเดียวกันหากอยู่ในประเทศไทยทั้งหมด ก็จะอยู่ภายใต้กฎหมาย PDPA เดียวกัน ในกรณีที่บริษัททั้งหมดในเครืออยู่ในประเทศไทย การแบ่งหรือใช้ข้อมูลร่วมกัน (Sharing) สามารถใช้ฐานเดียวกันได้ คือ ฐานสัญญา

การเปิดเผยข้อมูลออกไปยังบริษัทในเครือได้ จะต้องแจ้งกับพนักงานว่า อาจจะต้องมีการส่งข้อมูลออกไปให้กับบริษัทในเครือ หากบริษัทในเครือใช้นโยบายเรื่องการคุ้มครองข้อมูลส่วนบุคคล และนโยบายความเป็นส่วนตัวที่เป็นฉบับเดียวกันทั้งหมดก็ สามารถดำเนินการได้ แต่หากบริษัทในเครือมีนโยบายของตนเอง การแชร์ข้อมูลของพนักงาน จะต้องมีการตรวจสอบมาตรการ และขั้นตอน รวมทั้งมาตรฐานทางระบบก่อน

การแจ้ง Privacy Notice ตามมาตรา 23 ฐานทางกฎหมายที่ใช้ (Lawful Basis) **เป็นฐานสัญญา** จะต้องระบุให้ชัดเจนว่า จะเปิดเผยข้อมูลส่วนบุคคลอะไรบ้าง ไปยังบริษัทที่อยู่ในเครือบริษัทใด กรณีบริษัทในเครือแยกนโยบายคุ้มครองข้อมูลส่วนบุคคลกันคนละฉบับ ต้องแจ้งนโยบายของบริษัทในเครือให้พนักงานบริษัททราบด้วย

ความรับผิดชอบในฐานะ **“ผู้ควบคุมข้อมูลส่วนบุคคล”** เป็นของบริษัทต้นสังกัดที่พนักงานอยู่ในสังกัดในประเทศไทย จึงอยู่ในข้อบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลเช่นกัน

4.3.2 การใช้ข้อมูลพนักงานร่วมกันในเครือบริษัทที่อยู่ในต่างประเทศ

ในกรณีที่บริษัทในเครืออยู่ต่างประเทศ จะเข้ากับข้อกฎหมายตามมาตรา 28 และมาตรา 29 เพราะเมื่อส่งข้อมูลออกไปยังต่างประเทศ จำเป็นต้องมีการตรวจสอบประเทศปลายทางในส่วนของหลักการทางกฎหมาย โดยประเทศปลายทางจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกับประเทศไทยหรือไม่ด้อยไปกว่าของไทย ตัวอย่างเช่น การส่งข้อมูลจากประเทศในกลุ่มสหภาพยุโรป (Europe) ไปยังประเทศสิงคโปร์ หรือจากสหรัฐอเมริกาไปยังสหราชอาณาจักรและออสเตรเลีย กลุ่มประเทศเหล่านี้จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection) คล้ายกับประเทศไทย แต่หากส่งออกข้อมูลไปในประเทศที่ไม่มั่นใจในเรื่องของการคุ้มครองข้อมูล (Data Protection) จำเป็นต้องมีการตรวจสอบรายละเอียดก่อนทำการส่งข้อมูล

หากเป็นบริษัทในเครือของบริษัทสำนักงานใหญ่ โดยปกติจะมีเอกสารที่เรียกว่า กฎเกณฑ์ที่มีผลผูกพันขององค์กรธุรกิจ (Binding Corporate Rules: BCR) ซึ่งเป็นเสมือนกับเป็นบัญญัติที่ใช้กับทุก ๆ บริษัทในเครือ เช่น บริษัทแม่อยู่ญี่ปุ่นแต่มีสาขาย่อยทั่วโลก บริษัทลูกจะเปิดใช้บัญญัติฉบับเดียวกันและมีมาตรฐานในแนวทางเดียวกับบริษัทแม่ก็สามารถดำเนินการได้ แต่หากมีเหตุต้องส่งข้อมูลส่วนบุคคลออกไปในบริษัทที่ยังไม่

แน่ใจ จำเป็นต้องแจ้งให้พนักงานทราบว่าประเทศนี้ยังไม่มีมาตรฐานหรือยังไม่เปิดใช้งาน Data Protection เพื่อให้พนักงานได้ตัดสินใจก่อนจะเซ็นยินยอม

การแจ้ง Privacy Notice หรือ การแจ้งตามมาตรา 23 ฐานทางกฎหมายที่ใช้ (Lawful Basis) เป็นฐานสัญญา ระบุให้ชัดเจนว่าจะเปิดเผยข้อมูลส่วนบุคคลอะไรบ้าง ไปยังบริษัทมาตรฐานการรักษาความปลอดภัย Security Standard บริษัทผู้ส่งข้อมูลส่วนบุคคลออกไปยังต่างประเทศ ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ดีเพียงพอ (มาตรา 28, 29) บริษัทผู้ส่งข้อมูลส่วนบุคคลออกไปยังต่างประเทศ ต้องตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางถ้ายังไม่ดีเพียงพอ ต้องแจ้งเจ้าของข้อมูลส่วนบุคคล เพื่อขอความยินยอมก่อน ความรับผิดชอบในฐานะ **“ผู้ควบคุมข้อมูลส่วนบุคคล”** เป็นของบริษัทที่พนักงานสังกัดควรจัดทำเอกสาร Binding Corporate Rules (BCR)

4.3.3 การใช้ข้อมูลพนักงานร่วมกันระหว่างนายจ้าง กับ บริษัทจัดหาแรงงาน

ในบางกรณีการใช้ลูกจ้างเหมาค่าแรงแบบ Outsource อาจจะต้องใช้ข้อมูลจากทั้งสองฝ่าย ทั้งในส่วนของบริษัท Outsource และพนักงานเองซึ่งหากมีขั้นตอนการทำงานแบบนี้ ทางนายจ้างต้องมีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่คุ้มครองไปยังลูกจ้าง outsource ด้วย

1) มีกิจกรรมที่เกี่ยวข้องกับการ เก็บรวบรวม ใช้ หรือเปิดเผย และ ต่างฝ่ายต่างเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” Data Controller (DC)
2) ต่างฝ่ายต้องแจ้งตามมาตรา 23 (Privacy Notice) ให้พนักงานรับเหมาค่าแรงทราบ
3) ระหว่างนายจ้าง กับ บริษัทจัดหาแรงงาน ควรจัดทำ **“สัญญาแบ่งปันข้อมูล”** (Personal Data Sharing Agreement: DSA)

ความจำเป็นต้องใช้ แบ่งปัน โอน แลกเปลี่ยน หรือเปิดเผย (รวมเรียกว่า “แบ่งปัน”) ข้อมูลส่วนบุคคลที่ตนเก็บรักษาแก่อีกฝ่าย ซึ่งข้อมูลส่วนบุคคลที่แต่ละฝ่าย เก็บรวมรวม ใช้ หรือเปิดเผย (รวมเรียกว่า “ประมวลผล”) แต่ละฝ่ายต่างเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ แต่ละฝ่ายต่างเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบ และกำหนดวัตถุประสงค์ ในการประมวลผลข้อมูลส่วนบุคคลในข้อมูลที่ตนต้องแบ่งปัน

4.3.4 การใช้ข้อมูลพนักงานร่วมกันระหว่าง “ผู้ควบคุมข้อมูล” กับ “ผู้ประมวลผลข้อมูล”

การแบ่งปันข้อมูลระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลนั้นอยู่ในส่วนของมาตราต่าง ๆ เช่น การตรวจสุขภาพให้พนักงาน การส่งข้อมูลให้สถานพยาบาลที่รับตรวจ โดยการส่งต้องเป็นข้อมูลทั่วไป ไม่ใช่ข้อมูลที่อ่อนไหว เมื่อตรวจสุขภาพ นายจ้างควรให้พนักงานใช้แค่ รหัสพนักงาน ชื่อ - นามสกุล อายุ เท่านั้นในการเข้ารับการตรวจ

1) ฝ่ายหนึ่งเป็นผู้มีอำนาจสั่ง อีกฝ่ายต้องปฏิบัติตาม และไม่ตัดสินใจทำนอกเหนือคำสั่ง
2) ฝ่ายหนึ่งคือ “ผู้ควบคุมข้อมูล” กับอีกฝ่ายคือ “ผู้ประมวลผลข้อมูล”

3) ระหว่าง 2 ฝ่าย จัดทำ “สัญญาประมวลผลข้อมูลส่วนบุคคล” Data Processing Agreement (DPA)

มาตรา 40 วรรค 3

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

4.4 การประเมินผลงานของพนักงาน

การประเมินผลพนักงานโดยหลักที่เราพบเป็นประจำและใช้งานกันมีอยู่ 5 รายการ ดังนี้

4.4.1. การประเมินสัมภาษณ์งาน

เป็นการประเมินคุณสมบัติและคุณลักษณะเบื้องต้นสำหรับตำแหน่งงาน

4.4.2 การประเมินผลระยะทดลองงาน

ในทางปฏิบัติแล้วนั้นกำหนดระยะเวลาในการทดลองงานต้องไม่เกิน 119 วัน หากใช้ระยะเวลาถึง 120 วัน เมื่อเกิดการเลิกจ้างโดยเหตุไม่ผ่านการประเมิน นายจ้างจะต้องจ่ายค่าชดเชย ตาม พ.ร.บ.คุ้มครองแรงงาน มาตรา 118 อย่างไรก็ตาม ทาง HR ไม่ควรประเมินแค่ครั้งเดียวในวันที่ 119 แต่ควรประเมินกันในทุก 30 วัน 60 วัน และ 90 วัน

4.4.3 การประเมินผลงานประจำปี

การประเมินประจำปีนั้นอาจไม่ได้หมายความว่าในแต่ละปีจะมีการประเมินเพียงครั้งเดียว ในบางครั้งทางนายจ้างหรือ HR ก็จะมีการประเมินทุกไตรมาสที่ 1, 2, 3 และไตรมาสที่ 4 และรวมกันเป็นการประเมินผลงานประจำปี

4.4.4 การประเมินเพื่อปรับเลื่อนตำแหน่ง

การประเมินผลในรูปแบบนี้อาจจะต้องมีการนำผลการประเมินผลงานหลายปีย้อนหลัง เช่น 2-3 ปี หลังมาพิจารณาด้วยว่าได้มีผลการประเมินดีมาตลอดจึงควรได้รับการเลื่อนตำแหน่ง หรือเมื่อเลื่อนตำแหน่งไปแล้วพนักงานสามารถทำได้ตามตำแหน่งได้หรือไม่ และทำได้ตามความสามารถที่คาดหวังไว้หรือไม่

4.4.5 การประเมินเมื่อมีการเปลี่ยนงาน

เช่น พนักงานย้ายจากแผนกหนึ่งมาอีกแผนกหนึ่ง หรือ อาจจะย้ายการทำงานที่มีลักษณะใกล้เคียงกัน แต่อาจจะต้องมีการประเมินใหม่อีกครั้งว่าพนักงานยังมีศักยภาพในการทำงานเหมือนเดิมไหม

หลักการโดยทั่วไปของการประเมินผลพนักงานมี ประมาณ 5 เรื่อง ดังนี้

1) หัวข้อในการประเมินต้องเกี่ยวข้องกับการคัดเลือกคน
2) การให้ความคิดเห็นของกรรมการสัมภาษณ์ต้องระมัดระวัง
3) ไม่เปิดเผยให้ผู้ที่ไม่เกี่ยวข้องทราบถึงข้อมูล
4) เจ้าของข้อมูลส่วนบุคคลมีสิทธิตาม PDPA ในข้อมูลส่วนบุคคล
5) การทำลายเมื่อหมดความจำเป็น

4.4.6 กรณีตัวอย่างการประเมินพนักงาน

1. ตัวอย่างการประเมินหัวข้อเรื่องของการคัดเลือกพนักงาน

การคัดเลือกพนักงานจะมีการกำหนดคุณสมบัติที่นายจ้างต้องการ และมีพื้นที่ให้แสดงความคิดเห็นสำหรับผู้สัมภาษณ์ โดยปกตินั้นผู้สัมภาษณ์ก็ไม่ใช่แค่ HR ฝ่ายเดียว แต่ก็จะมีผู้จัดการฝ่าย หรือหัวหน้าฝ่ายนั้น ๆ เข้าร่วมในการสัมภาษณ์ด้วย เพราะฉะนั้นจุดที่สำคัญคือเมื่อเราการคัดเลือกคนเข้าทำงาน ประเด็นคำถามควรเป็นหัวข้อที่สัมพันธ์กับการทำงานและการเขียนความคิดเห็นที่หัวหน้าเขียนก็จะต้องสัมพันธ์กับตำแหน่งการทำงานเช่นกัน ซึ่งผู้สมัครที่เข้ารับการสัมภาษณ์มีสิทธิในการขอดูใบประเมินได้ว่าเหตุใดจึงไม่ผ่านการสัมภาษณ์งาน

ตัวอย่างจากต่างประเทศ มีอาจารย์ท่านหนึ่งประเมินคะแนนนักเรียน แต่เด็กคนนี้ประเมินไม่ผ่าน และยังมีเด็กอีกสี่คนที่ประเมินไม่ผ่านเช่นกัน โดยกลุ่มเด็กทั้ง 4 มาหาอาจารย์เพื่อขอดูข้อสอบที่อาจารย์ให้คะแนนและแสดงความคิดเห็นว่าทำไมเขาถึงไม่ผ่าน โดยอาจารย์นั้นต้องให้ดู แต่เด็กทั้ง 4 ไม่ได้ดูพร้อมกัน ไม่เห็นคะแนนของกันและกัน เมื่อนำมาเทียบเคียงกันกับเรื่องของการประเมินการสัมภาษณ์งาน ผู้เข้าร่วมสัมภาษณ์มีสิทธิที่จะขอดูแบบประเมินเช่นกัน เพราะฉะนั้นในการออกแบบแบบประเมินจะต้องมีความสอดคล้องกับเรื่องของงานเท่านั้น ไม่ว่าจะเป็นสัมภาษณ์งาน ประเมินงาน ทดลองงานหรือประเมินการผ่านงานแล้ว และการแสดงความคิดเห็นควรจะอยู่ในกรอบของการทำงาน

ในเรื่องของการประเมินผลงานประจำปีก็จะมีเนื้อหาที่ใกล้เคียงกัน แบบฟอร์มควรมีการระบุเป็นหัวข้อและในช่องที่เป็นตัวเลขให้ใช้คำ ว่า “พอใช้”“ดี” “ดีมาก” และไม่ควรใช้ว่า “ดีมากกว่า” “ดีมาก” “ดี” “พอใช้” “ควรปรับปรุง” ซึ่งรูปแบบนี้เราก็ต้องมีหลักฐานและมีการแสดงความคิดเห็นที่ถูกต้องตามเรื่องของการทำงาน โดยส่วนมากการประเมินเราจะต้องให้ feedback กับพนักงานว่าต้องพัฒนาอะไร และเมื่อมีการให้ Feedback ขั้นตอนต่อไปคือการให้ความรู้ความเข้าใจกับทางหัวหน้างานว่าพนักงานนั้นมีสิทธิในการที่จะขอดู

ผลการประเมิน เพราะฉะนั้นเวลาดำเนินการจะต้องโปร่งใสและเป็นธรรม โดยผลการประเมินต่าง ๆ ควรมีการเก็บประมาณ 2-3 ปี

4.5 การบันทึกเวลาของพนักงานในรูปแบบต่าง ๆ

ในสมัยก่อนนั้นการบันทึกเวลาจะเป็นในรูปแบบของบัตรตอก การรูดบัตร และการใส่รหัส ซึ่งปัจจุบันมีเทคโนโลยีใหม่ ๆ เกิดขึ้นตลอดเวลา เช่น

1) Finger Scan (การสแกนลายนิ้วมือ)
2) Face Recognition (การจดจำใบหน้า)
3) Iris (รูม่านตา)
4) Voice Recognition (การจดจำเสียง)
5) การสแกนเส้นเลือดดำบนฝ่ามือ

ข้อมูลทั้งหมดนี้ถือเป็นข้อมูลทางชีวภาพ (Biometric) ซึ่งเป็นข้อมูลละเอียดอ่อนที่จำเป็นต้องปกป้องสูงกว่าข้อมูลทั่วไป เนื่องจากใช้ในการปลอมแปลงตัวตนได้ การเก็บข้อมูลเหล่านี้จัดอยู่ในมาตรา 26 ที่ห้ามมิให้เก็บข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อ ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล

การสแกนลายนิ้วมือ (Finger Scan) เสถียรภาพไม่ค่อยดี สามารถปลอมแปลงได้ง่ายกว่า การจดจำใบหน้า Face Recognition ในขณะที่การสแกนรูม่านตา ก็พัฒนาขึ้น สามารถแบ่งแยกฝาแฝดได้ เนื่องจากโครโมโซมไม่เหมือนกัน แต่การสแกนรูม่านตาบ่อย ๆ อาจส่งผลต่อม่านตาได้ จึงไม่ค่อยใช้ในอุตสาหกรรมหรือองค์กรทั่วไป ในขณะที่การสแกนเสียง Voice recognition ก็สามารถทำได้ง่าย แต่ไม่เสถียรเช่นเดียวกัน เนื่องจากเสียงสามารถเปลี่ยนได้ในสภาวการณ์ต่าง ๆ เช่น อารมณ์เสีย หรือไม่สบาย เป็นต้น ส่วนการสแกนเส้นเลือดดำบนฝ่ามือ ถือเป็นเทคโนโลยีล่าสุด

อย่างไรก็ตาม มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

4.6 การเก็บข้อมูลเพื่อบันทึกเวลาการเข้างาน

กรณี **“ไม่ต้องขอความยินยอม”** : บัตรตอก บัตรรูด ใส่รหัส ลงสมุดเข้างาน

กรณี **“ต้องขอความยินยอม”** : Biometric สแกนนิ้วมือ สแกนใบหน้า สแกนม่านตา

กรณีศึกษาฐานทางกฎหมายที่ใช้ในการบันทึกเวลาทำงานของพนักงาน

องค์กรนายจ้างบางแห่ง มีโรงงานหลายแห่ง และมีวิศวกรหลายคน ซึ่งทำงานไม่พร้อมกัน และทำให้ต้องมีรถประจำตำแหน่งเพื่อสะดวกในการเดินทาง นายจ้างจึงมีการติด GPS ในรถ เพื่อดูรายงานการเข้าออกงาน ในกรณีดังกล่าวสามารถดำเนินการโดยใช้ ฐานประโยชน์อันชอบธรรม (Legitimate Interest) เนื่องจากมีเหตุผลที่เพียงพอและพอรับได้ว่าเพื่อใช้ในการคิดค่าทำงานล่วงเวลา แต่ในกรณีนี้ข้อควรระวัง คือ จะทำอย่างไรเพื่อไม่ให้เป็นการละเมิดความเป็นส่วนตัวหลังเลิกงาน วิธีที่ดีที่สุด คือ ปิดการติดตาม GPS ตอนเลิกงาน แต่อาจเป็นเรื่องยุ่งยากพอสมควร ดังนั้นการขอความยินยอม จึงเป็นอีกแนวทางหนึ่งในการดำเนินการในกรณีดังกล่าว โดยจะต้องออกแบบขั้นตอนในการเก็บข้อมูลให้ดี เพื่อให้พนักงานมั่นใจว่าจะไม่เกิดการละเมิดสิทธิ์ส่วนบุคคล

ในการขอความยินยอมนั้น สามารถขอความยินยอมในวันทำสัญญาเข้าทำงาน โดยความยินยอมจะต้องไม่เป็นส่วนใดส่วนหนึ่งของสัญญา เช่น การแยกเอกสารขอความยินยอมโดยเฉพาะ เพื่อให้มั่นใจว่าความยินยอมนั้นไม่ใช่ส่วนหนึ่งของสัญญาและในการขอความยินยอมสามารถอธิบายถึงความจำเป็นต้องเก็บโดยแต่ละองค์กรอาจมีเอกสารขอความยินยอมที่แตกต่างกัน ทั้งนี้ ในการขอความยินยอมสามารถแบ่งออกเป็นเรื่อง ๆ เช่น การเก็บข้อมูลด้านสุขภาพ ขอความยินยอมข้อมูลการตรวจประวัติอาชญากรรม ขอความยินยอมในการสแกนใบหน้าเพื่อรายงานการเข้าออกสำนักงานและนอกจากหนังสือขอความยินยอมเมื่อเข้าทำงานแล้ว ในกรณีที่พนักงานลาออกควรลบทำลายข้อมูลทันทีเมื่อหมดความจำเป็น นายจ้างอาจจะต้องเตรียมแบบฟอร์มและขั้นตอนการขอถอนความยินยอมในกรณีที่พนักงานต้องการ โดยจะต้องออกแบบให้ง่ายเหมือนกับการขอความยินยอมตอนเข้าทำงานเช่นกัน

4.7 การตรวจสุขภาพของพนักงานและใบรับรองแพทย์

การตรวจสุขภาพของพนักงานถือเป็นสิ่งที่สำคัญเพราะนอกจากจะเป็นหน้าที่หลักของงาน HR แล้ว การตรวจสุขภาพ ยังเป็นเกี่ยวข้องกับข้อมูลอ่อนไหว มีด้วยกันหลายประเภท ดังนี้

1. ตรวจสุขภาพก่อนเข้างาน
2. ตรวจสุขภาพโรคตามงานเสี่ยง
3. ตรวจสุขภาพประจำปี
4. ตรวจสารเสพติด
5. ใบรับรองแพทย์ประกอบการลาป่วย
6. ใบรับรองแพทย์ประกอบสิทธิสวัสดิการ
7. ใบรับรองแพทย์เบิกประกันสังคมกองทุนทดแทน
8. ใบรับรองแพทย์เบิกประกันสังคมกองทุนประกันสังคม
9. ใบรับรองแพทย์เบิกประกันชีวิต

ข้อมูลสุขภาพ และ พระราชบัญญัติโรคติดต่อ พ.ศ. 2557 (จำเป็นในการตรวจสุขภาพ)

“โรคติดต่อ” หมายความว่า โรคที่เกิดจากเชื้อโรคหรือพิษของเชื้อโรคซึ่งสามารถแพร่โดยทางตรงหรือทางอ้อมมาสู่คน

“โรคติดต่ออันตราย” หมายความว่า โรคติดต่อที่มีความรุนแรงสูงและสามารถแพร่ไปสู่ผู้อื่นได้อย่างรวดเร็ว

“โรคติดต่อที่ต้องเฝ้าระวัง” หมายความว่า โรคติดต่อที่ต้องมีการติดตาม ตรวจสอบ หรือจัดเก็บ ข้อมูลอย่างต่อเนื่อง

“โรคระบาด” หมายความว่า โรคติดต่อหรือโรคที่ยังไม่ทราบสาเหตุของการเกิดโรคแน่ชัด ซึ่งอาจแพร่ไปสู่ผู้อื่นได้อย่างรวดเร็วและกว้างขวาง หรือมีภาวะของการเกิดโรคมากผิดปกติกว่าที่เคยเป็นมา

การขอใบรับรองแพทย์จากลูกจ้าง

ตาม พ.ร.บ.คุ้มครองแรงงาน พ.ศ. 2541 นายจ้างขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่หากกรณีลาป่วยไม่เกิน 3 วัน และนายจ้างขอใบรับรองแพทย์จากลูกจ้างหรือ กรณีนายจ้างขอใบรับรองแพทย์เพื่อนำไปใช้วัตถุประสงค์อย่างอื่น จำเป็นจะต้องจัดทำหนังสือขอความยินยอม

4.8 การให้สวัสดิการกับการเก็บข้อมูลส่วนบุคคล

สวัสดิการนั้นเป็นส่วนหนึ่งในการจูงใจให้พนักงานทำงานกับนายจ้างและยังช่วยให้รับพนักงานใหม่ได้ง่ายขึ้น สวัสดิการนั้นอยู่นอกเหนือกฎหมาย ขึ้นอยู่กับแต่ละองค์กร ซึ่งในปัจจุบันแต่ละองค์กรมีสวัสดิการมากมาย ซึ่งมีส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. สวัสดิการแต่งงาน คลอดบุตร งานศพ

ในส่วนนี้ต้องดูว่านายจ้างมีขั้นตอนในการดำเนินงานการเบิกจ่ายสวัสดิการอย่างไร ถ้าให้เบิกได้เลยโดยไม่ต้องใช้เอกสารใด ๆ จะไม่มีส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่ถ้าต้องมีเอกสารแนบ เช่น สูติบัตร ถือเป็นการเก็บข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์ จึงจำเป็นต้องมีการขอความยินยอม ซึ่งผู้ปกครองส่วนใหญ่ย่อมอยากจะได้สวัสดิการและยินดีในการให้ความยินยอม หรือในกรณีพนักงานแต่งงานหากทางนายจ้างต้องใช้ทะเบียนสมรสเป็นหลักฐาน ถือเป็นการเก็บข้อมูลส่วนบุคคลของบุคคลที่สาม ซึ่งต้องใช้การขอความยินยอมเช่นกัน

2. การท่องเที่ยวประจำปี การแข่งกีฬา งานเลี้ยงปีใหม่งานเลี้ยงเกษียณ

ส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ การถ่ายรูป ทั้งนี้คนไทยส่วนใหญ่จะชอบการถ่ายรูป แต่อาจจะมีบางคนที่ไม่ชอบให้มีการเผยแพร่ในสื่อต่าง ๆ ดังนั้นจึงจะต้องเคารพสิทธิของคนกลุ่ม

ดังกล่าว จึงควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคล ไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆ เช่น การขอลบ เป็นต้น

3. งานเลี้ยงวันเกิดแจกของ

ในแต่ละเดือน นายจ้างบางแห่งจะมีการเปิดเผยชื่อพนักงานที่เกิดในเดือนนั้น ๆ และการจัดกิจกรรมวันเกิด ซึ่งอาจจะมีบางคนที่ไม่ต้องการให้มีการเปิดเผยเช่นกัน ดังนั้น จึงควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคล ไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆ

4. กองทุนสำรองเลี้ยงชีพ

ในส่วนของกองทุนสำรองเลี้ยงชีพนั้น ส่วนใหญ่จะแค่เปิดเผยข้อมูลไปยังผู้จัดการกองทุนเท่านั้น ซึ่งเป็นข้อมูลทั่วไป จึงไม่ค่อยมีประเด็นเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล

5. การลาพิเศษในวันสำคัญทางศาสนา

ในการเก็บข้อมูลทางศาสนากรณีที่มีความจำเป็น เช่น เพื่อให้วันหยุดเพิ่มตามศาสนา ทั้งนี้ นายจ้างสามารถขอความยินยอมให้พนักงานให้ข้อมูลหลังจากได้รับการคัดเลือกเป็นพนักงาน เพื่อเป็นสิทธิประโยชน์ในการลาของพนักงาน แต่อย่างไรก็ตาม พนักงานมีสิทธิที่จะให้หรือไม่ให้ก็ได้ แต่ไม่จำเป็นต้องขอความยินยอมตั้งแต่ตอนสมัคร เพราะจะส่งผลต่อการจัดการในกรณีที่ผู้สมัครงานไม่ได้รับการคัดเลือก

ทั้งนี้ หากเป็นกรณีมีการจัดกิจกรรมที่ต้องจัดเตรียมอาหาร จัดห้องพิเศษ เช่น เพื่อการละหมาด นายจ้างไม่จำเป็นต้องขอข้อมูลทางศาสนา แต่สามารถถามความต้องการในเรื่องของสิ่งอำนวยความสะดวกเพิ่มเติม แล้วให้พนักงานแจ้งเอง โดยเลี่ยงการขอข้อมูลทางศาสนา

6. ค่าเดินทางหรือจัดรถรับส่ง

การให้ค่าเดินทาง หรือการจัดรถรับส่งพนักงาน นายจ้างควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคลไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆ เช่น ขอเก็บข้อมูล ที่อยู่บ้าน หรือตำแหน่งบ้าน โดยมีเหตุผลรองรับ คือ เพื่อให้ HR สามารถจัดการระบบการรับส่งพนักงาน เส้นทางการเดินรถ จำนวนรถได้ ซึ่งถือเป็นสวัสดิการอย่างหนึ่งของนายจ้าง

7. สวัสดิการห้องพยาบาลที่มีแพทย์หรือพยาบาล

ในกรณีที่นายจ้างหรือโรงงานขนาดใหญ่มีแพทย์และพยาบาลซึ่งเป็นพนักงานของนายจ้างเอง ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เดียวกัน อาจจะบริหารจัดการได้ง่าย แต่ถ้าใช้แพทย์หรือพยาบาลบุคคลภายนอก (Outsource) ถือเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ในการเก็บข้อมูลส่วนบุคคลด้านสุขภาพ แพทย์และพยาบาลมีความจำเป็นต้องคุ้มครองข้อมูลสุขภาพของพนักงาน ซึ่งถือ

เป็นข้อมูลส่วนบุคคลอ่อนไหว ดังนั้น จึงต้องมีการทำความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้แก่แพทย์และพยาบาลด้วย

ในกรณีที่นายจ้างมีสวัสดิการมากกว่าสวัสดิการที่กล่าวมาข้างต้น นายจ้างจะต้องพิจารณาว่าเข้าข่ายกฎหมายมาตราใด และจะต้องขอความยินยอมหรือดำเนินการอย่างไรเพื่อให้สอดคล้องกับกฎหมายอีกด้วย

8. การฝึกอบรมให้พนักงาน

ในการฝึกอบรม ไม่มีการเก็บข้อมูลส่วนบุคคลอ่อนไหว จะใช้เฉพาะข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล ตำแหน่ง เบอร์โทร อีเมล์ เป็นต้น โดยการฝึกอบรมพนักงานสามารถแยกออกเป็น 2 ประเภท คือ การฝึกอบรมในประเทศ และการฝึกอบรบต่างประเทศ ดังนี้

การฝึกอบรมในประเทศ สามารถแบ่งได้เป็น

1) Public Training

เป็นการส่งพนักงานไปฝึกอบรมภายนอกองค์กร ซึ่งจะต้องมีการเปิดเผย ชื่อ นามสกุล ตำแหน่ง เบอร์โทรศัพท์ อีเมล์ มีการลงทะเบียนหน้าห้องก่อนเข้าอบรม

2) In-House Training

เป็นการจัดฝึกอบรมภายในองค์กร ซึ่งจะต้องมีการเปิดเผย ชื่อ นามสกุล ตำแหน่ง แผนก รวมทั้งมีการบันทึกภาพระหว่างการอบรม ซึ่งการฝึกอบรมภายในไม่ได้มีผลกระทบกับเรื่องการคุ้มครองข้อมูลส่วนบุคคลมากนัก เพราะอยู่ภายในองค์กร

3) Online Training

การฝึกอบรมออนไลน์ ในปัจจุบันสามารถขึ้นทะเบียนขอรับรองหลักสูตรกับกรมพัฒนาฝีมือแรงงานได้ โดยจะต้องเก็บข้อมูลส่วนบุคคล เช่น ใบหน้า ซึ่งต้องบันทึกภาพการอบรมไว้ตลอดการฝึกอบรม ในการฝึกอบรมแบบออนไลน์นั้นมีเรื่องที่ต้องคำนึงถึง คือ เรื่องความปลอดภัย (Security) นายจ้างควรจะต้องรู้ว่าใช้ผู้ให้บริการ (Provider) ของใคร ซึ่งในการเลือกใช้ ควรจะเลือกใช้ที่ได้รับการรับรองว่าได้ขึ้นทะเบียนความปลอดภัย (Security) กับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแล้ว ระบบออนไลน์สามารถบันทึกได้ และคุ้มครองข้อมูลส่วนบุคคลได้ รู้ว่า server เก็บไว้ที่ใด มีระบบการคุ้มครองดี และสามารถตรวจสอบได้ ทั้งนี้ในส่วนของการขึ้นทะเบียนรับรองหลักสูตรกับกรมพัฒนาฝีมือแรงงาน กรณีที่มีพนักงาน 100 คนขึ้นไป จะต้องมีการเปิดเผย ชื่อ นามสกุล แผนก และรหัสบัตรประชาชน ของผู้เข้าอบรม ซึ่งเป็นไปตามฐานกฎหมาย เนื่องจากมีกฎหมายในเรื่องดังกล่าวอยู่แล้ว

การฝึกอบรมต่างประเทศ

ในกรณีที่นายจ้างต้องส่งพนักงานเพื่อไปฝึกอบรมที่ต่างประเทศ ไม่ว่าจะเป็น Public Training หรือ In-House Training ที่สำนักงานใหญ่ ในส่วนของการคุ้มครองข้อมูลส่วนบุคคล จะเกี่ยวข้องกับ Privacy Notice หรือการแจ้งตามมาตรา 23 โดยใช้ฐานสัญญาได้ ซึ่งเป็นการส่งข้อมูลส่วนบุคคลแบบทั่วไป

ข้อควรคำนึง คือ ระบบความมั่นคงปลอดภัย (security) ของประเทศปลายทาง ซึ่งควรจะต้องมีระบบที่ดี มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มแข็ง และการปฏิบัติตามได้เหมือนของไทย เพื่อความมั่นใจในการส่งข้อมูลส่วนบุคคลออกไป ทั้งนี้ในการส่งข้อมูลส่วนบุคคลออกไปต่างประเทศ ควรพิจารณาตามมาตรา 28-29 ซึ่งหากมาตราฐานของประเทศปลายทางไม่ดีเพียงพอ นายจ้างควรจะต้องแจ้งเจ้าข้อมูลส่วนบุคคลเพื่อขอความยินยอมก่อน เพราะหากเกิดปัญหา นายจ้างจะต้องเป็นผู้รับผิดชอบคนแรก ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

4.9. การจ้างแรงงานต่างด้าว กับการเก็บข้อมูลส่วนบุคคล

แรงงานต่างด้าวที่ทำงานในไทยนั้นมีหลายแบบ ทั้งในระดับผู้บริหาร และระดับแรงงาน ที่ส่วนใหญ่จะเป็นแรงงานต่างด้าวตาม MOU คือ พม่า กัมพูชา ลาว ซึ่งไม่ว่าจะมาจากประเทศใดล้วนจำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น ไม่ว่าประเทศนั้น ๆ จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ในฐานะที่นายจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ในการเข้ามาทำงานในประเทศไทยนั้น ก่อนที่จะเดินทางเข้าประเทศ แรงงานต่างด้าวจะต้องมีการส่งข้อมูลส่วนตัว เช่น ทะเบียนบ้าน สำเนาพาสปอร์ตเพื่อให้นายจ้างได้นำไปใช้ในการยื่นเรื่อง เพื่อให้แรงงานต่างด้าวสามารถขอวีซ่าเข้าประเทศ รวมไปถึงการทำใบอนุญาตทำงาน (Work Permit) ซึ่งหากแรงงานต่างด้าวอยู่ในประเทศไทยเกิน 90 วัน ก็จะต้องมีการยื่นเรื่องแจ้งกองตรวจคนเข้าเมืองทุก ๆ 90 วัน กระบวนการเหล่านี้ล้วนเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งสิ้น

การตรวจสุขภาพแรงงานต่างด้าว

ถึงแม้ว่าจะไม่มีกฎหมายหรือข้อบังคับให้นายจ้างสามารถทำการตรวจสุขภาพก่อนเข้างานได้ ยกเว้นกลุ่มธุรกิจอาหารที่พนักงานจะต้องมีการสัมผัสกับอาหารตามกฎหมายว่าด้วยการสาธารณสุข แต่สำหรับแรงงานต่างด้าว จะสามารถตรวจสุขภาพก่อนเข้างานได้ตามกฎหมายว่าด้วยการตรวจสุขภาพของแรงงานต่างด้าว โดยจะต้องมีใบรับรองแพทย์ 7 โรคด้วยกัน เพื่อใช้ในการยื่นขอใบอนุญาตทำงาน (Work Permit) ซึ่งในกรณีนี้นายจ้างสามารถดำเนินการขอข้อมูลส่วนบุคคลประเภทอ่อนไหวได้ตามฐานกฎหมาย โดยไม่ต้องขอความยินยอม

ในการดำเนินการเพื่อให้แรงงานต่างด้าวทำงานในประเทศไทยนั้น HR ต้องเป็นผู้ไปยื่นเอกสารต่าง ๆ กับหน่วยงานราชการหรือจ้าง Outsource เป็นผู้ดำเนินการ ซึ่งจะต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งหมด ถ้าดำเนินการโดยพนักงานของนายจ้าง ข้อมูลก็จะไหลเวียนอยู่ในองค์กร แต่หากมีการจ้าง outsource นายจ้างจำเป็นต้องให้ Outsource ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลด้วย เพราะหาก Outsource ไม่มีความรู้ อาจเกิดละเมิดได้ โดยเฉพาะในกรณีที่แรงงานต่างด้าวมาจากประเทศในกลุ่ม EU

หรือสหรัฐอเมริกา ซึ่งให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว โดยในการคัดเลือก Outsource อาจต้องคัดเลือกองค์กรที่มีระบบคุ้มครองข้อมูลส่วนบุคคลที่ถูกต้องและดีพอ ซึ่งจะสามารถตรวจสอบได้ง่ายกว่า การใช้บุคคลธรรมดา ซึ่งอาจจะต้องให้ความรู้เกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ต้องมีการทำข้อตกลงประมวลผลข้อมูล (Data Processing Agreement: DPA) อีกด้วย เพราะ Outsource ถือเป็น ผู้ประมวลผลข้อมูล (Data Processor)

4.10 สหภาพแรงงานกับการเก็บข้อมูลส่วนบุคคล

ในประเภทนายจ้างที่มีสหภาพแรงงาน จะเกี่ยวข้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ **ข้อมูลสหภาพแรงงาน** ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด **โดยไม่ได้รับความยินยอม**โดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

ซึ่งหากนายจ้างมีการสอบถามว่าใครเป็นสมาชิกสหภาพแรงงาน จะเข้าข่ายกฎหมายมาตราดังกล่าว คือ ต้องมีการขอความยินยอม สหภาพแรงงานนั้นถือเป็นอีกนิติบุคคลหนึ่งที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ต้องมีนโยบายความเป็นส่วนตัว (Data Protection Policy) ที่เอาไปใช้กับสมาชิกของสหภาพแรงงาน และหากต้องมีกิจกรรมไหนที่ต้องขอความยินยอมสมาชิกก็จะต้องดำเนินการเช่นกัน ซึ่งบทบาทของนายจ้างกับสหภาพแรงงานอาจจะแตกต่างกัน

กรณีศึกษากิจกรรมหักค่าบำรุงสมาชิก

ใน พ.ร.บ.คุ้มครองแรงงาน ตามมาตรา 76 นั้น นายจ้างสามารถหักค่าบำรุงสมาชิกเพื่อชำระให้แก่สหภาพแรงงานได้ ซึ่งสหภาพแรงงานจะต้องมีข้อตกลงหรือข้อเรียกร้องมายังนายจ้างให้ช่วยหักค่าสมาชิกของพนักงานดังรายชื่อที่จัดส่งมาให้ โดยทางสหภาพแรงงานจะต้องเป็นผู้ขอความยินยอมกับสมาชิกโดยตรง เนื่องจากสหนภาพแรงงานมีบทบาทเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ในขณะที่นายจ้างจะทำหน้าที่ในส่วนของผู้ประมวลผล (Data Processor) คือดำเนินการหักค่าบำรุงสมาชิกตามที่สหภาพแรงงานแจ้งมาเท่านั้น นายจ้างไม่สามารถดำเนินการอื่นใดเพิ่มเติมจากข้อตกลงได้

4.11 กิจกรรมสอบสวนทางวินัย

กรณีที่สหภาพแรงงานมีข้อเรียกร้อง เช่น ในกรณีที่สมาชิกของสหภาพแรงงานทำผิดระเบียบวินัยและมีการตั้งคณะกรรมการสอบสวน หนึ่งในคณะกรรมการสอบสวนนั้น จะต้องเป็นคณะกรรมการของสหภาพแรงงานหรือคณะกรรมการลูกจ้าง

หากนายจ้างจะมีการลงโทษพนักงาน นายจ้างจะต้องแจ้งพนักงานว่าหากเป็นสมาชิกสหภาพฯ ให้ไปแจ้งสหภาพฯ เพื่อให้สหภาพฯ มาแจ้งนายจ้าง เพื่อเชิญสหภาพฯ มาเป็นคณะกรรมการสอบสวน ไม่ว่านายจ้างจะทราบหรือไม่ว่าพนักงานรายนั้นเป็นสมาชิกของสหภาพฯ หรือไม่ นายจ้างจะไม่เป็นผู้ขอความยินยอมเองแต่จะให้สหภาพฯ ขอความยินยอมแล้วจึงมาแจ้งนายจ้าง

4.12. กิจกรรมแจ้งข้อเรียกร้องตาม พ.ร.บ.แรงงานสัมพันธ์ มาตรา 13 และมาตรา 15

พ.ร.บ.แรงงานสัมพันธ์ มาตรา 13 จะแตกต่างจากมาตรา 15 ดังนี้

มาตรา 13 ลูกจ้างสามารถยื่นข้อเรียกร้องไปที่นายจ้างได้ ในกรณีที่ลูกจ้างไม่ได้เป็นสหภาพฯ โดยมีการรวมตัวกัน 15% ของพนักงาน ระบุรายชื่อกับลายมือชื่อยื่นมาที่นายจ้างเพื่อขอเรียกร้อง ในกรณีนี้สามารถทำได้

มาตรา 15 ถ้าเป็นกลุ่มสหภาพแรงงาน ตัวแทนสหภาพแรงงานสามารถยื่นข้อเรียกร้องมาที่นายจ้างได้โดยไม่ต้องแสดงรายชื่อสมาชิก ซึ่งหากนายจ้างสงสัยว่าจำนวนสมาชิกไม่ครบตามที่กฎหมายกำหนด ก็สามารถทำเรื่องขอตรวจสอบรายชื่อกับกรมสวัสดิการคุ้มครองแรงงาน ซึ่งกรมฯก็จะไม่เปิดเผยรายชื่อเช่นกัน แต่จะแจ้งว่าครบตามจำนวนที่กฎหมายกำหนดหรือไม่

4.13 แนวปฏิบัติเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูล

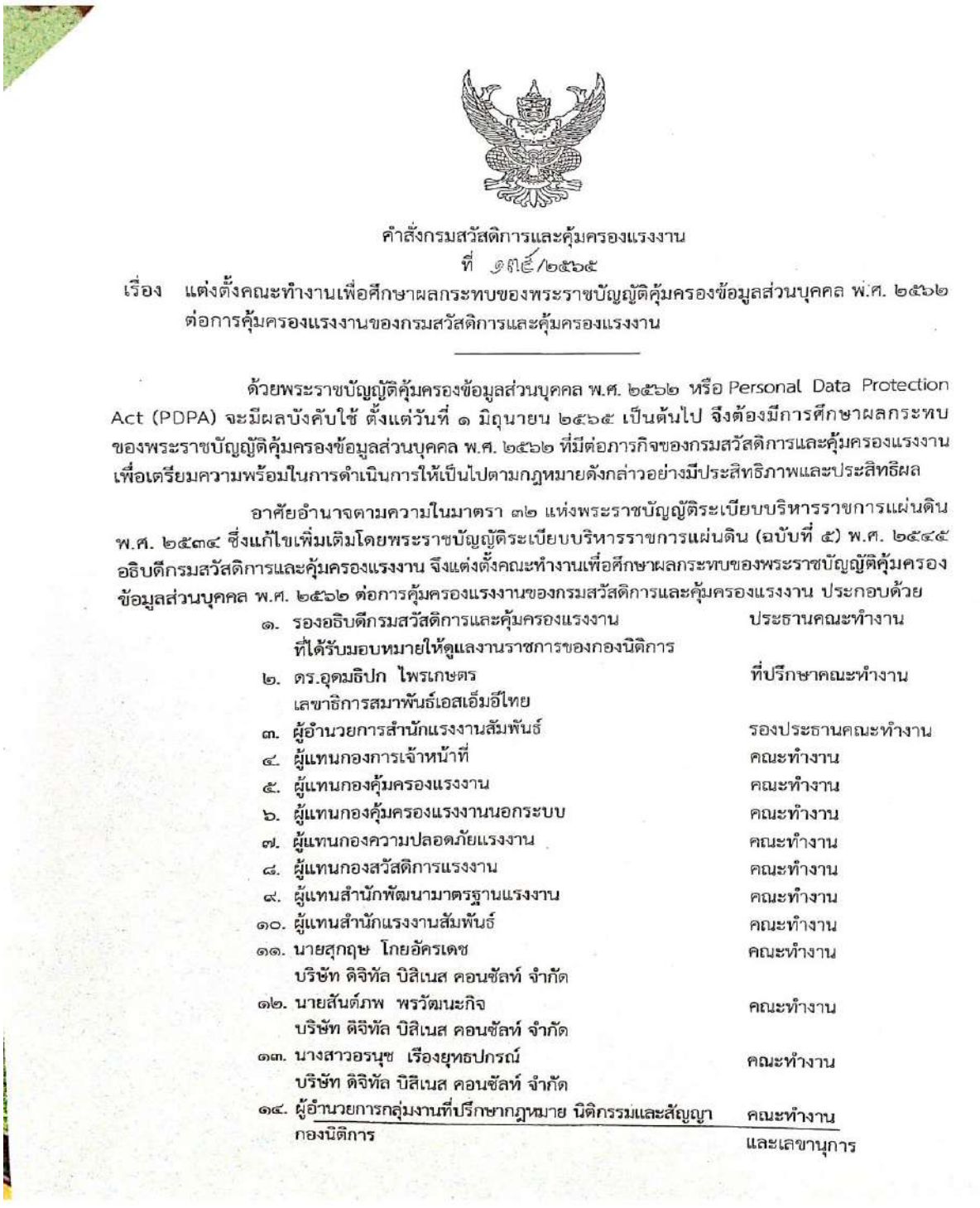
การจัดเก็บข้อมูลและเอกสารส่วนบุคคล เป็นมาตรการที่ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลต้องปฏิบัติตามข้อกำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคล ส่วนเงื่อนไขระยะเวลานั้น เป็นการกำหนดได้เองโดยนโยบายของนายจ้าง โดยใช้หลักการและพื้นฐานทางกฎหมายสำหรับเรื่องหรือเอกสารนั้น ๆ หรือฐานกฎหมายเฉพาะประเภทธุรกิจที่กำหนดไว้ เช่น ธนาคาร สถาบันการเงิน ประกันภัย เป็นต้น

ข้อกฎหมายสำหรับอายุความในกรณีต่าง ๆ

ประเด็น	อายุความ	มาตรา
กรณีลูกจ้างฟ้องเรียกค่าจ้าง	2 ปี	ปพพ. ม.193/34
กรณีลูกจ้างฟ้องเรียกค่าจ้างในช่วงเวลาที่นายจ้างสั่งพักงาน	2 ปี	ปพพ. ม.193/34
กรณีลูกจ้างฟ้องค่าทำงานล่วงเวลา / ค่าล่วงเวลาในวันหยุด	2 ปี	ปพพ. ม.193/34
กรณีลูกจ้างฟ้องเรียกเงินอื่นที่ไม่ใช่ค่าจ้าง	10 ปี	ปพพ. ม.193/30
กรณีฟ้องเรียกค่าเสียหายเนื่องจากการผิดสัญญาจ้างแรงงาน	10 ปี	ปพพ. ม.193/30
กรณีนายจ้างใช้สิทธิไล่เบี้ยจากลูกจ้างที่นายจ้างชดใช้ให้แก่บุคคลภายนอก	10 ปี	ปพพ. ม.193/30
กรณีลูกจ้างฟ้องเรียกค่าชดเชยจากนายจ้าง	10 ปี	ปพพ. ม.193/30
กรณีลูกจ้างฟ้องเรียกดอกเบี้ยค้างชำระ / ดอกเบี้ยของค่าชดเชย	5 ปี	ปพพ. ม.193/33 (1)
กรณีลูกจ้างฟ้องเรียกค่าจ้างแทนการบอกกล่าวล่วงหน้า	10 ปี	ปพพ. ม.193/30
กรณีฟ้องเรียกค่าเสียหายจากการละเมิดสัญญาจ้างแรงงาน	1 ปี	ปพพ. ม.448

ภาคผนวก

1. คำสั่งแต่งตั้งคณะทำงาน กรมสวัสดิการและคุ้มครองแรงงาน



คำสั่งกรมสวัสดิการและคุ้มครองแรงงาน
ที่ ๑๓๕/๒๕๖๕

เรื่อง แต่งตั้งคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต่อการคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงาน

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือ Personal Data Protection Act (PDPA) จะมีผลบังคับใช้ ตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ เป็นต้นไป จึงต้องมีการศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่มีต่อภารกิจของกรมสวัสดิการและคุ้มครองแรงงาน เพื่อเตรียมความพร้อมในการดำเนินการให้เป็นไปตามกฎหมายดังกล่าวอย่างมีประสิทธิภาพและประสิทธิผล

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน จึงแต่งตั้งคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต่อการคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงาน ประกอบด้วย

๑. รองอธิบดีกรมสวัสดิการและคุ้มครองแรงงาน ที่ได้รับมอบหมายให้ดูแลงานราชการของกองนิติการ	ประธานคณะทำงาน
๒. ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย	ที่ปรึกษาคณะทำงาน
๓. ผู้อำนวยการสำนักแรงงานสัมพันธ์	รองประธานคณะทำงาน
๔. ผู้แทนกองการเจ้าหน้าที่	คณะทำงาน
๕. ผู้แทนกองคุ้มครองแรงงาน	คณะทำงาน
๖. ผู้แทนกองคุ้มครองแรงงานนอกระบบ	คณะทำงาน
๗. ผู้แทนกองความปลอดภัยแรงงาน	คณะทำงาน
๘. ผู้แทนกองสวัสดิการแรงงาน	คณะทำงาน
๙. ผู้แทนสำนักพัฒนามาตรฐานแรงงาน	คณะทำงาน
๑๐. ผู้แทนสำนักแรงงานสัมพันธ์	คณะทำงาน
๑๑. นายสุกฤษ โกยอัครเดช บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัด	คณะทำงาน
๑๒. นายสันต์ภพ พรวัฒนะกิจ บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัด	คณะทำงาน
๑๓. นางสาวอรนุช เรืองยุทธปกรณ์ บริษัท ดิจิทัล บิสิเนส คอนซัลท์ จำกัด	คณะทำงาน
๑๔. ผู้อำนวยการกลุ่มงานที่ปรึกษากฎหมาย นิติกรรมและสัญญา กองนิติการ	คณะทำงานและเลขานุการ

สแกนด้วย CamScanner

๑๕. นิติกรระดับชำนาญการขึ้นไป กองนิติการ คณะทำงานและผู้ช่วยเลขานุการ

ให้คณะทำงานมีอำนาจหน้าที่ ดังนี้

๑. พิจารณาและศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่มีต่อภารกิจของกรมสวัสดิการและคุ้มครองแรงงาน

๒. จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของกรมสวัสดิการและคุ้มครองแรงงาน เพื่อเป็นแนวปฏิบัติให้สถานประกอบกิจการให้มีการดำเนินการที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. ๒๕๔๑ และกฎหมายอื่นๆ ที่อยู่ในความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

๓. สนับสนุนและเผยแพร่แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของกรมสวัสดิการและคุ้มครองแรงงาน แก่นายจ้าง ลูกจ้าง และผู้มีส่วนเกี่ยวข้อง

๔. ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

สั่ง ณ วันที่ ๕ มีนาคม พ.ศ. ๒๕๖๕

(นายนิยม สองแก้ว)
อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน

คำสั่งกรมสวัสดิการและคุ้มครองแรงงาน
ที่ ๒๙๑/๒๕๖๕
เรื่อง แต่งตั้งคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต่อการคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงานเพิ่มเติม

ตามที่กรมสวัสดิการและคุ้มครองแรงงานมีคำสั่ง ที่ ๑๓๕/๒๕๖๕ ลงวันที่ ๘ มีนาคม พ.ศ. ๒๕๖๕ แต่งตั้งคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต่อการคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงาน นั้น

เนื่องจากคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เห็นชอบแต่งตั้งบุคลากรที่มีความเชี่ยวชาญเป็นคณะทำงานเพิ่มเติม เพื่อเป็นการเตรียมความพร้อมในการดำเนินการให้เป็นไปตามกฎหมายอย่างมีประสิทธิภาพและประสิทธิผล อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน จึงมีคำสั่งแต่งตั้งคณะทำงานเพื่อศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ต่อการคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงานเพิ่มเติม ประกอบด้วย

๑. ผศ.ดร.ธีรัต ชวิศจินดา ผู้อำนวยการศูนย์กฎหมายเพื่อการพัฒนา สถาบันบัณฑิตพัฒนบริหารศาสตร์	คณะทำงาน
๒. นายนรเทพ บุญเก็บ ประธานคณะกรรมการพัฒนากฎหมายธุรกิจ และช่วยเหลือผู้ประกอบการ mSMEs สมาพันธ์เอสเอ็มอีไทย	คณะทำงาน
๓. นายเกรียงไกร สินบัวทอง ผู้อำนวยการสถาบันพัฒนาและทดสอบทักษะดิจิทัล	คณะทำงาน
๔. นายทรงพล หนูบ้านเกาะ Consultant & Auditor Manager สถาบันพัฒนาและทดสอบทักษะดิจิทัล	คณะทำงาน
๕. นางสาวดวงดาว สำนองสุข PDPA Consultant & Auditor PDPA Thailand	คณะทำงาน
๖. นางสาวมยุรี ชวนชม PDPA Consultant & Auditor PDPA Thailand	คณะทำงาน
๗. นายกฤตพล ศรีระษา PDPA Consultant & Auditor PDPA Thailand	คณะทำงาน

- ๒ -

ให้คณะทำงานมีอำนาจหน้าที่ ดังนี้

๑. พิจารณาและศึกษาผลกระทบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่มีต่อภารกิจของกรมสวัสดิการและคุ้มครองแรงงาน

๒. จัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของกรมสวัสดิการและคุ้มครองแรงงาน เพื่อเป็นแนวปฏิบัติให้สถานประกอบกิจการให้มีการดำเนินการที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. ๒๕๔๑ และกฎหมายอื่นๆ ที่อยู่ในความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

๓. สนับสนุนและเผยแพร่แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของกรมสวัสดิการและคุ้มครองแรงงาน แก่นายจ้าง ลูกจ้าง และผู้มีส่วนเกี่ยวข้อง

๔. ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

สั่ง ณ วันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๕

(นายนิยม สองแก้ว)
อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน

2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

https://www.krisdika.go.th/librarian/get?sysid=834296&ext=htm

3. ข้อมูลพระราชบัญญัติคุ้มครองแรงงาน

https://www.krisdika.go.th/librarian/get?sysid=642571&ext=htm

4. พระราชกฤษฎีกากำหนดลักษณะ กิจการ หรือหน่วยงาน ที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566

https://ratchakitcha.soc.go.th/documents/140A048N0000000004500.pdf

5. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

5.1 การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565

https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0024.PDF

5.2 หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0026.PDF

5.3 มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0028.PDF

5.4 หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565

https://ratchakitcha.soc.go.th/documents/17211327.pdf

5.5 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566

https://ratchakitcha.soc.go.th/documents/140D174S0000000006400.pdf

5.6 การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) พ.ศ. 2566

https://ratchakitcha.soc.go.th/documents/140D226S0000000001200.pdf

DBC Group | PDPA THAILAND | ddti | pdpa dpo SERVICE

PDPA THAILAND

ให้คำปรึกษา พร้อมจัดทำ PDPA & DPO ครบวงจร โดยทีมผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

เมื่อความไม่รู้ ความไม่เข้าใจ PDPA อย่างแท้จริง
ทำให้เกิดความเสี่ยงที่จะทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ปิดจุดอ่อน แก้ไขข้อผิดพลาด ด้วยบริการของเรา

PDPA&DPO Consultant

ให้คำปรึกษาทางด้านกฎหมาย การบริหารจัดการ
กระบวนการการทำงาน และซอฟต์แวร์ที่เกี่ยวข้อง
กับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Auditor

ตรวจสอบเอกสาร กระบวนการการทำงาน
กระบวนการบริหารจัดการ และเทคโนโลยี
ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

PDPA&DPO Tools

จัดหาเครื่องมือที่จำเป็นในการปฏิบัติตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
เช่น Consent, RoPA, DSRM และ DPIA เป็นต้น

DPO Outsource

ให้บริการเป็น
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือ
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

PDPA&DPO In-House Training

ให้บริการอบรมภายใน ด้วยหลักสูตรบรรยาย
และ Workshop ที่ออกแบบเฉพาะธุรกิจของคุณ
โดยผู้เชี่ยวชาญจากสถาบันพัฒนาและทดสอบ
ทักษะดิจิทัล (DDTI)

PDPA&DPO e-Learning

หลักสูตรออนไลน์ที่ออกแบบเนื้อหา
เกี่ยวกับ PDPA อย่างครบถ้วนและครอบคลุม
ช่วยให้พนักงานเข้าใจ PDPA อย่างง่ายดาย
สะดวก และประหยัดเวลา

บริษัท ดีบีซี กรุ๊ป จำกัด

เลขที่ 125/55 ซอยวิภาวดีรังสิต 60 แยก 12 แขวงตลาดบางเขน เขตหลักสี่ กรุงเทพฯ 10210
+66(0)2-029-0707 กด 1-5
+66(0)81-632-5918
pdpa@dbcgroup.asia
PDPA Thailand
PDPA Thailand
www.dbcgroup.asia

www.pdpathailand.com

LINE @pdpathailand

สนับสนุนโดย