แนวปฏิบัติตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการ

V5 (09.05.2023)

สารบัญ

สารบัญ

เรื่อง **หน้า**

คำนำ

เอกสารแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการฉบับนี้ จัดทำขึ้นเพื่อให้สถานประกอบการที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงานได้นำไปใช้เพื่อประกอบการดำเนินกิจกรรมของสถานประกอบการที่เกี่ยวกับข้อมูลส่วนบุคคลของบุคลากรให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

เอกสารฉบับนี้จะเกิดขึ้นมิได้ หากไม่ได้รับการสนับสนุนจาก นายนิยม สองแก้ว อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน ดร.อุดมธิปก ไพรเกษตร เลขาธิการสมาพันธ์เอสเอ็มอีไทย ที่ปรึกษาคณะทำงาน และความร่วมแรง ร่วมใจ จากคณะทำงานของกรมสวัสดิการและคุ้มครองแรงงาน รวมไปถึงหน่วยงานที่เกี่ยวข้องที่ทำให้เกิดเอกสารฉบับนี้ โดยเฉพาะอาจารย์สุกฤษ โกยอัครเดช, อาจารย์สันต์ภพ พรพัฒนะกิจ, อาจารย์มยุรี ชวนชม, อาจารย์ดวงดาว สำนองสุข, อาจารย์ณัฏฐ์ ธนวนกุล รวมถึงท่านอื่น ๆ ที่มิได้เอ่ยนามมา ณ ที่นี้

ด้วยเงื่อนไขของเวลาและข้อจำกัดทางกฎหมายที่ได้มีการเริ่มประกาศใช้ หากท่านมีข้อสังเกต ข้อแลกเปลี่ยนความคิดเห็น ตลอดจนข้อติชมต่าง ๆ หรือ หากมีข้อผิดพลาดประการใด สามารถแนะนำได้ที่ pdpasme@smethai.or.th และสามารถศึกษาข้อมูลเพิ่มเติมได้ที่ https://smethai.or.th/?page_id=6253 เพื่อที่จะนำมาใช้ในการปรับปรุงและพัฒนาเอกสารแนวปฏิบัติการคุ้มครองแรงงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ให้เป็นประโยชน์กับทุกฝ่ายต่อไป

กรมสวัสดิการและคุ้มครองแรงงาน

สมาพันธ์เอสเอ็มอีไทย

PDPA Thailand

สถาบันพัฒนาและทดสอบทักษะดิจิทัล (DDTI)

20 กรกฎาคม 2565

ความเป็นมา

เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2565 ซึ่งเป็นกฎหมายใหม่ที่มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดยที่เจ้าของข้อมูลส่วนบุคคลนั้นจะเป็นบุคคลธรรมดาที่อาศัยอยู่ในประเทศไทย อันเป็นสาเหตุให้ผู้ใช้แรงงาน พนักงาน และลูกจ้าง นั้นต่างก็เป็นเจ้าของข้อมูลส่วนบุคคล และมีความจำเป็นที่จะต้องได้รับการคุ้มครองข้อมูลส่วนบุคคลของตนเอง

ขณะเดียวกันกฎหมายฉบับนี้มุ่งเน้นให้นิติบุคคลต้องดำเนินการเพื่อให้เกิดความสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล มิเช่นนั้น จะมีโทษตามกฎหมาย เป็นเหตุให้สถานประกอบการซึ่งอยู่ภายใต้กฎหมายคุ้มครองแรงงานของกรมสวัสดิการและคุ้มครองแรงงาน เกิดความวิตกกังวลที่จะต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองแรงงาน และพระราชบัญญัติอื่น ๆ ที่อยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

ทางสมาพันธ์เอสเอ็มอีไทย ซึ่งเป็นองค์กรเอกชนที่ไม่แสวงหาผลกำไร อันเกิดจากการรวมตัวกันของผู้ประกอบการเอสเอ็มอีไทยจำนวนกว่า 100,000 ราย (www.smethai.or.th) เล็งเห็นถึงความสำคัญในเรื่องดังกล่าว จึงได้ร่วมกับพันธมิตรของสมาพันธ์ฯ ที่มีความเชี่ยวชาญและมีความชำนาญในเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกรมสวัสดิการและคุ้มครองแรงงานจัดตั้งคณะทำงานฯ ขึ้นเพื่อจัดทำแนวปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับการคุ้มครองแรงงานสำหรับสถานประกอบการขึ้น เพื่อให้เกิดประโยชน์ต่อสถานประกอบการซึ่งอยู่ภายใต้ความรับผิดชอบของกรมสวัสดิการและคุ้มครองแรงงาน

เนื่องจากกฎหมายฉบับนี้มีความจำเป็นที่จะต้องมีกฎหมายระดับรองอีกจำนวนมาก รวมทั้งการบังคับใช้เมื่อเกิดสถานการณ์จริง โดยที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำลังเร่งจัดทำรายละเอียดต่างๆเพิ่มเติม ซึ่งผู้อ่านสามารถติดตามความคืบหน้าและรายละเอียดของกฎหมายระดับรองและการบังใช้กฎหมายฉบับนี้ได้ที่ www.pdpc.or.th

คณะทำงานหวังเป็นอย่างยิ่งว่า เอกสารที่ได้จัดทำขึ้นนี้จะเป็นประโยชน์ต่อผู้ใช้แรงงาน พนักงาน และลูกจ้างในสถานประกอบการ ตลอดจนเป็นแนวทางให้สถานประกอบการสามารถนำไปปรับใช้ในการดำเนินกิจกรรมเพื่อให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่อไป และเนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายใหม่จึงมีความจำเป็นที่จะต้องปรับปรุงและพัฒนาแนวปฏิบัตินี้ให้สมบูรณ์ยิ่งขึ้นในภายภาคหน้า

PDPA สำคัญอย่างไร ทำไม HR ต้องรู้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Privacy Data Protection Act - PDPA) เป็นกฎหมายใหม่ที่เรียกได้ว่ามีผลกระทบต่อทุกๆ องค์กร โดยเฉพาะฝ่ายทรัพยากรบุคคล หรือ HR ทุกบริษัท เนื่องจากมีแนวโน้มเป็นหน่วยงานที่มีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล มากที่สุดในองค์กร เพราะต้องบริหารจัดการข้อมูลทั้งของพนักงานภายใน รวมถึงข้อมูลของผู้สมัครงาน และพนักงานที่ออกจากจากองค์กรไปแล้ว

ตัวอย่างข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ HR

- ชื่อ นามสกุล ที่อยู่ รายละเอียดติดต่อ ของพนักงาน ตั้งแต่ระดับปฏิบัติการจนถึงระดับบริหาร
- Resume หรือ CV ของผู้สมัครงานที่ยื่นเข้ามายังองค์กร
- บันทึกประวัติการทำงานของผู้ที่ออกจากองค์กรไปแล้ว (อาจย้ายงาน ลาออก หรือถูกไล่ออก) เก็บรักษาไว้เป็นฐานข้อมูลในกรณีมีการสอบถามเข้ามาจากองค์กรสังกัดใหม่ของพนักงาน
- ข้อมูลติดต่อประสานงานวิทยากรจากภายนอกสำหรับงานฝึกอบรม

สำหรับบริษัทใหญ่ๆ อาจมีงบประมาณในการจ้างที่ปรึกษา ผู้เชี่ยวชาญ หรือบริการบริหารจัดการ เข้ามาช่วยจัดการวางระบบ Flow ของข้อมูล ตลอดจนการ Storage ให้สอดคล้องกับ PDPA และมีความปลอดภัยสูงสุด แต่สำหรับองค์กรเล็ก SMEs หรือบริษัทที่เพิ่งตั้งตัวอาจมีงบประมาณไม่มาก ผู้บริหารตลอดจนเจ้าหน้าที่ฝ่าย HR จึงจำเป็นต้องเรียนรู้เกี่ยวกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และดำเนินงานขององค์กรให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วยตนเอง

HR ทุกบริษัท ควรคำนึงถึงจุดใดบ้าง เพื่อดำเนินการตาม PDPA?

สำหรับชาว HR ต้องคำนึงว่าข้อมูลในมือของพวกคุณมีโอกาสเป็นข้อมูลส่วนบุคคลได้เสมอ และข้อมูลเหล่านี้ล้วนอยู่ภายใต้การคุ้มครองจาก PDPA (และกฎหมายอย่าง GDPR รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับอื่นๆ หากมีการโอนถ่ายข้อมูลจากหรือไปยังองค์กรในต่างประเทศ) จึงจำเป็นต้องมีนโยบายเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลที่เขียนไว้เป็นลายลักษณ์อักษรอย่างชัดเจน โดยมีตัวอย่างแนวทางการปฏิบัติงานของฝ่ายทรัพยากรบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ที่คุณอาจนำไปปรับใช้ได้ ดังนี้

- ก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล HR ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แม้เรซูเม่/ประวัติโดยย่อของบุคคลจะถูกส่งมาจากผู้สมัครงานโดยตรง ซึ่งอาจตีความได้ว่าเป็นการให้ความยินยอมแล้ว แต่ยังคงต้องมีการแจ้งและให้ยอมรับเกี่ยวกับการเก็บรักษาข้อมูลนั้นเอาไว้เป็นฐานข้อมูลในกรณีที่การสมัครงานไม่ผ่านตามที่คาดหวัง และไม่เก็บข้อมูลนั้นไว้เกินระยะเวลาที่ระบุตามนโยบายการประมวลผลข้อมูลขององค์กร
- ฝ่ายบุคคลยังไม่ควรขอข้อมูลบัตรประชาชนจากผู้สมัครงาน ไม่ว่าจะเป็นตัวจริงหรือสำเนา จนกระทั่งผ่านกระบวนการพิจารณาและได้ตำแหน่งงานในบริษัทอย่างเป็นทางการ
- เรซูเม่/ประวัติของผู้ที่ไม่ผ่านการสมัครงานควรถูกเก็บรักษาเอาไว้แค่เพียงระยะสั้น ๆ และควรมีขั้นตอนในการทำลายข้อมูลนั้นอย่างปลอดภัย
- ก่อนมีการส่งต่อข้อมูลของผู้สมัครงานเพื่อพิจารณาในตำแหน่งงานอื่น ๆ นอกเหนือจากตำแหน่งที่ผู้สมัครงานระบุว่ามีความประสงค์ จะต้องมีการขอความยินยอมเสียก่อน โดย HR ควรแจ้งในประกาศรับสมัครงานว่าทางบริษัทจะมีการส่งต่อข้อมูลของบุคคลสำหรับการพิจารณาตำแหน่งงานอื่น ๆ ที่เกี่ยวข้องให้กับผู้สมัครงานด้วย ตาม PDPA คุณจะต้องเขียนข้อความเพื่อขอความยินยอมในส่วนนี้แยกออกมาจากส่วนอื่นให้ชัดแจ้ง และอาจให้ผู้สมัครงานเซ็นต์ยอมรับในจุดนี้แยกอีกครั้งหนึ่งด้วย
- ฝ่ายบุคคลต้องมีนโยบายเกี่ยวกับการเก็บรักษา และมาตรการทำลายข้อมูลส่วนบุคคลของอดีตบุคลากรที่ชัดเจน
- หากบริษัทหรือองค์กรของคุณมีความจำเป็นในการคอยตรวจสอบสังเกตการณ์การทำงานของบุคลากรผ่านอีเมล การใช้งานคอมพิวเตอร์ และโทรศัพท์ กรณีดังกล่าวจะต้องมีการแจ้งให้บุคลากรผู้เป็นเจ้าของข้อมูลรับทราบพร้อมระบุถึงเหตุผลของการดำเนินการดังกล่าว

บทที่ 1

ที่มาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและความสัมพันธ์กับกฎหมายคุ้มครองแรงงาน

1. ที่มาของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

วันที่ 25 พฤษภาคม พ.ศ.2561 ได้มีการประกาศการบังคับใช้กฎหมาย GDPR หรือ General Data Protection Regulation ในสหภาพยุโรป โดยมีวัตถุประสงค์เพื่อป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบ กฎหมาย GDPR นั้น บังคับใช้กับทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ในสหภาพยุโรป ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน กล่าวคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในสหภาพยุโรป ไม่ว่าการประมวลผลจะทำในสหภาพยุโรปหรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นในสหภาพยุโรป

นอกจากมีผลบังคับใช้ภายในประเทศสมาชิกสหภาพยุโรปแล้วยังส่งผลถึงผู้ประกอบการในประเทศไทยที่จะต้องดำเนินการติดต่อสื่อสาร หรือ รับส่งข้อมูลส่วนบุคคลของประชากรในประเทศที่เป็นสมาชิกของสหภาพยุโรป (Cross-Border Data Transfer Issues) โดยผู้ประกอบการในไทยจำเป็นต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอด้วยในการดำเนินการต่าง ๆ ทางธุรกิจที่มีการเก็บข้อมูลส่วนบุคคล

ประเทศไทยกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

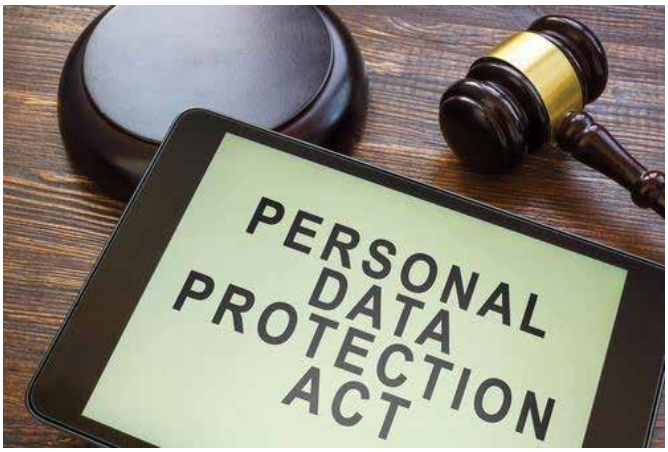
1 ปีต่อมา หลังจากที่สหภาพยุโรปได้มีการประกาศใช้ GDPR หรือ General Data Protection Regulation ไปแล้วนั้น ประเทศไทยก็ได้มีการประกาศในราชกิจจานุเบกษา ในวันที่ 27 พฤษภาคม 2562 เพื่อกำหนดให้หน่วยงาน หรือ กิจการที่มีการประมวลผล อันได้แก่ การเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้อยู่ภายใต้การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ “PDPA” ซึ่งย่อมาจาก Personal Data Protection Act B.E.2019 (2562) โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุให้องค์กรหรือหน่วยงานที่เกี่ยวข้องในการดำเนินการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของประชาชนไม่ว่าจะเป็นบริษัทเอกชน หรือ หน่วยงานภาครัฐ จะต้องไม่นำเอาข้อมูลส่วนบุคคลของประชาชนไปใช้ในกิจกรรมอื่น ๆ ที่ไม่ได้รับความยินยอมหรือฐานทางกฎหมายอื่น และกฎหมายดังกล่าวได้มีการบังคับใช้อย่างเต็มรูปแบบแล้ว เมื่อวันที่ 1 มิถุนายน พ.ศ.2565

กฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่บัญญัติขึ้นโดยมีวัตถุประสงค์ในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป โดยมีเจตนารมณ์ที่จะคุ้มครองข้อมูลส่วนบุคคลของประชาชนในสภาวการณ์ที่การใช้งานข้อมูลส่วนบุคคลกลายเป็นเรื่องที่จำเป็นและมีความสำคัญในทุกภาคส่วนไม่ว่าจะเป็นหน่วยงานของรัฐหรือองค์กรธุรกิจภาคเอกชน ผลของความจำเป็นดังกล่าวอาจส่งผลต่อเจ้าของข้อมูลส่วนบุคคล เช่น การโทรขายสินค้าหรือการแลกเปลี่ยนข้อมูลเพื่อประโยชน์ทางธุรกิจที่อาจกระทบถึงความเป็นส่วนตัวในชีวิตประจำวันของบุคคล เป็นต้น

บทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลลักษณะที่มีความพิเศษแตกต่างจากกฎหมายฉบับอื่น กล่าวคือ กฎหมายไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่บทบัญญัติจะมุ่งเน้นสร้างความตระหนักรู้ การทบทวนและกลไกในการพิจารณาเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต่างๆเพื่อให้การกระทำใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวภายใต้หลักการของกฎหมาย

2. เจตนารมณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

PDPA ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019) เป็นกฎหมาย ว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคล โดยมีสร้างมาตรฐานในการรักษาความปลอดภัยและความเป็นส่วนตัวข้อมูลส่วนบุคคล ให้มีการนำไปใช้อย่างตรงตามวัตถุประสงค์ และตรงตามความยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้อนุญาต โดยกฎหมาย PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ได้มีการประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และมีการผลบังคับใช้อย่างเต็มรูปแบบในวันที่ 1 มิถุนายน 2565



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นไม่เพียงแต่เข้ามาเป็นมาตรฐานด้านความปลอดภัยและการใช้ข้อมูล แต่ยังเป็นการส่งเสริมและสนับสนุนให้เกิดการใช้ประโยชน์ของข้อมูลส่วนบุคคลอย่างปลอดภัยและเป็นไปตามมาตรฐานสากล นอกจากนี้ประเทศไทยยังมีนโยบายเศรษฐกิจดิจิทัล หรือ Thailand Digital Economy Policy เพื่อส่งเสริมและผลักดันให้เกิดเศรษฐกิจดิจิทัล แต่ประเด็นที่เกี่ยวกับความมั่นคงปลอดภัย หรือ Data Protection ในส่วนของ Cybersecurity E-commerce ของประเทศไทยนั้นยังมีความอ่อนแอ จึงจำเป็นอย่างยิ่งที่จะต้องหันมาให้ความสำคัญในเรื่องนี้

2.1 ความเป็นส่วนตัวของข้อมูล หรือ Information Privacy

ความเป็นส่วนตัวของข้อมูล หรือ Information Privacy หมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่นโดยสิทธินี้ใช้ได้อย่างครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล และองค์กรหรือหน่วยงานต่าง ๆ

การละเมิดข้อมูลส่วนบุคคลในสังคมไทยและการฟ้องร้องนั้นเกิดขึ้นมาอย่างยาวนานโดยที่ยังไม่มี พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และหากจะฟ้องร้องเรื่องการละเมิดความเป็นส่วนตัวนั้น จะอยู่ในหัวข้อเรื่องของ“ความเป็นส่วนตัว” (Privacy) และสามารถฟ้องในประมวลกฎหมายแพ่งและพาณิชย์ตาม มาตรา 420

2.2 ทำไมจึงต้องมีกฎหมาย PDPA

2.2.1 **การละเมิดข้อมูลส่วนบุคคล** เนื่องจากที่ผ่านมามีการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากอันส่งผลให้เกิดความเดือดร้อนหรือส่งผลให้เกิดความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลนั้น

2.2.2 **เทคโนโลยีสารสนเทศ** ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีสารสนเทศเป็นสาเหตุสำคัญที่ทำให้ การเก็บ รวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลนั้นเกิดปัญหาในการถูกละเมิดได้โดยง่าย และรวดเร็วซึ่งก่อให้เกิดความเสียหายทั้งต่อตัวบุคคลและต่อเศรษฐกิจโดยรวม

2.2.3 **กฎหมาย** มีการกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

2.3 การป้องกันข้อมูลส่วนบุคคล

“ข้อมูลส่วนบุคคล” หรือ Personal Data คือ ข้อมูลที่เกี่ยวข้องกับบุคคลอันจะสามารถระบุตัวตน ของบุคคลนั้น ๆ ได้ ทั้งทางตรงและทางอ้อม เว้นแต่กรณีข้อมูลของผู้เสียชีวิตจะไม่นับเป็นข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคลจะแบ่งออกเป็น 2 ประเภท ดังนี้

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data)
หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล หรือชื่อเล่น / เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล) / ที่อยู่, อีเมล, เลขโทรศัพท์ / ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน / ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง / ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคลเช่น log file / ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต	หมายถึง ข้อมูลที่เป็นเรื่องส่วนบุคคลโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและอาจสุ่มเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เป็นข้อมูลส่วนบุคคลอีกประเภท ที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ฉบับนี้ให้ความสำคัญและมีบทลงโทษที่รุนแรงในกรณีเกิดการละเมิด ได้แก่ ข้อมูลเชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ, หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

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

2.4 ขอบเขตการบังคับใช้กฎหมาย PDPA (Law Enforcement)

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือ PDPA บังคับใช้กับใครบ้าง

2.4.1 **ผู้ควบคุมข้อมูล** หรือ **ผู้ประมวลผลข้อมูล** ที่ “อยู่ในราชอาณาจักร” ไม่ว่าการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลนั้นจะกระทำ **“ใน”** หรือ **“นอก”** ราชอาณาจักรก็ตาม

2.4.2 **ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลที่ “อยู่นอกราชอาณาจักร”** แต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ของข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในราชอาณาจักร โดยมีการดำเนินกิจกรรม ดังนี้

(1) มีการเสนอสินค้าหรือบริการ ให้แก่เจ้าของข้อมูล (ไม่ว่าจะมีการชำระเงินหรือไม่) ในราชอาณาจักร

(2) มีการเฝ้าติดตามพฤติกรรม ของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้น ในราชอาณาจักร

กรณีศึกษา 1 : กรณีที่ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อยู่ในประเทศไทย ได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคนที่อยู่ในประเทศไทย กรณีนี้บริษัทนั้นจะต้องอยู่ภายใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

กรณีศึกษา 2 : กรณี ที่บริษัทอยู่ต่างประเทศ มีการก่อตั้งอยู่นอกราชอาณาจักรไทย ตัวอย่างเช่น Google, Line, Facebook กรณีนี้จะดำเนินการอยู่ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) หากที่มีการนำเสนอการขายสินค้าหรือบริการหรือเฝ้าติดตามพฤติกรรม ให้กับเจ้าของข้อมูลในราชอาณาจักร (ไม่จำกัดสัญชาติ) โดยต้องแต่งตั้งตัวแทนในประเทศไทย

ดังนั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA จึงมีผลในการบังคับใช้กับบุคคลและหน่วยงานต่าง ๆ ทั้งหมด เช่น ผู้ประกอบการ – เจ้าของธุรกิจ หุ้นส่วน คู่ค้า ลูกค้า – ผู้บริโภค พนักงาน – ลูกจ้าง หรือ หน่วยงานภาครัฐ

2.5 ความสัมพันธ์ระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกฎหมายคุ้มครองแรงงาน

หลังจากที่กฎหมายได้มีการประกาศใช้อย่างเป็นทางการเต็มรูปแบบแล้ว ในวันที่ 1 มิถุนายน พ.ศ. 2565 กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เข้าไปมีบทบาทสำคัญอย่างมากในทุกๆอุตสาหกรรม ที่มีการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในแง่ของการคุ้มครองแรงงาน มีกิจกรรมต่างๆ และข้อมูลของพนักงานที่กฎหมายดังกล่าเข้าไปเกี่ยวข้อง โดยไม่จำกัดเพียงแค่ภาครัฐเท่านั้น แต่ยังรวมไปถึงภาคเอกชนที่มีการประมวลผลข้อมูลของพนักงานภายในองค์กรด้วย ในแง่ของการคุ้มครองแรงงาน กฎหมายที่สำคัญที่เข้ามาเกี่ยวข้อง คือ กฎหมายคุ้มครองแรงงาน ไม่ว่าจะเป็นกิจกรรมการคัดเลือกพนักงาน การทำสัญญาจ้างแรงงาน การพัฒนาบุคคลกร การอนุมัติเลื่อนตำแหน่ง หรือแม้แต่การพ้นสภาพการจ้างของพนักงาน กฎหมายดังกล่าวได้เข้าไปมีความเกี่ยวพันทุกกระบวนการ ตัวอย่างเช่น ในกิจกรรมการจัดทำทะเบียนลูกจ้างตามพระราชบัญญัติคุ้มครองแรงงาน มาตรา 115 ได้มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้จัดเก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดการจ้าง จะเห็นได้ชัดว่า การกำหนดระยะเวลาการทำลายข้อมูลดังกล่าวตามกฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดรายละเอียดการทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการดำเนินการลบ หรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว โดยเป็นไปตามหลัก การจัดเก็บข้อมูลอย่างจำกัด (storage minimization) หรือ กิจกรรมที่เกี่ยวกับการขอลาของพนักงาน กฎหมายคุ้มครองแรงงาน ได้มีการกำหนดให้นายจ้างสามารถขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่ถ้าเป็นกรณีที่ลาไม่เกิน 3 วันหรือกรณีที่นำไปใช้เพื่อวัตถุประสงค์อื่น นายจ้างมีหน้าที่ต้องขอความยินยอมจากลูกจ้าง เป็นต้น

บทที่ 2

นิยามและบุคคลที่เกี่ยวข้องเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน

1. นิยามของข้อมูลส่วนบุคคล

1.1 ข้อมูลส่วนบุคคล (Personal Data)

หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล ชื่อเล่นลูกจ้าง หมายเลขโทรศัพท์ลูกจ้าง เลขประจำตัวประชาชนลูกจ้างเลขหนังสือเดินทาง 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) ข้อมูลแฝง (Pseudonymous Data) หรือข้อมูลผู้ถึงแก่กรรม เป็นต้น

1.2 ข้อมูลส่วนบุคคลละเอียดอ่อน (Sensitive Data) หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งบริษัทต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ โดยบริษัทจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อน ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือในกรณีที่บริษัทมีความจำเป็นต้องดำเนินการตามที่กฎหมายอนุญาต เช่น การเก็บข้อมูลประวัติอาชญากรรมของลูกจ้าง บริษัทไม่สามารถเก็บได้ เว้นแต่ได้รับความยินยอมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือ เว้นแต่เข้าข้อยกเว้นที่กฎหมายกำหนด หรือในกรณีของการเก็บข้อมูลของใบรับรองแพทย์ ซึ่งมีข้อมูลสุขภาพ บริษัทไม่สามารถเก็บได้เว้น เว้นแต่ได้รับความยินยอม หรือเว้นแต่เข้าข้อยกเว้นตามกฎหมาย

2. บุคคลที่เกี่ยวข้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน

2.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น แต่ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของข้อมูล (Ownership) หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดย **เจ้าของข้อมูลส่วนบุคคล** (Data Subject) นี้จะหมายถึงบุคคลธรรมดาเท่านั้น และไม่รวมถึง “นิติบุคคล” (Juristic Person) ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท สมาคม มูลนิธิ หรือองค์กรอื่นใด ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลได้แก่ บุคคลดังต่อไปนี้

2.1.1 เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะ หมายถึง

- บุคคลที่มีอายุตั้งแต่ 20 ปีบริบูรณ์ขึ้นไป
- ผู้ที่สมรสตามกฎหมายตั้งแต่อายุ 17 ปีบริบูรณ์ขึ้นไป
- ผู้ที่สมรสก่อนอายุ 17 ปี โดยศาลอนุญาตให้ทำการสมรส
- ผู้เยาว์ซึ่งผู้แทนโดยชอบธรรมให้ความยินยอมในการประกอบธุรกิจทางการค้าหรือธุรกิจอื่น หรือในการทำสัญญาเป็นลูกจ้างในสัญญาจ้างแรงงาน ในความเกี่ยวพันกับการประกอบธุรกิจหรือ การจ้างแรงงานข้างต้นให้ผู้เยาว์มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว

ทั้งนี้ ในการให้ความยินยอมใด ๆ เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้บรรลุนิติภาวะสามารถให้ความยินยอมได้ด้วยตนเอง

2.1.2 เจ้าของข้อมูลส่วนบุคคลที่เป็น “ผู้เยาว์” หมายถึง บุคคลที่อายุต่ำกว่า 20 ปีบริบูรณ์ และไม่ใช่ผู้บรรลุนิติภาวะตามข้อ 2.1.1 ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

2.1.3 เจ้าของข้อมูลส่วนบุคคลที่เป็นคน “เสมือนไร้ความสามารถ” หมายถึงบุคคลที่ศาลสั่งให้เป็นคนเสมือนไร้ความสามารถเนื่องจากมีกายพิการหรือมีจิตฟั่นเฟือนไม่สมประกอบ หรือประพฤติสุรุ่ยสุร่ายเสเพลเป็นอาจิณหรือติดสุรายาเมา หรือมีเหตุอื่นใดทำนองเดียวกันนั้น จนไม่สามารถจะจัดทำการงานโดยตนเองได้ หรือจัดกิจการไปในทางที่อาจจะเสื่อมเสียแก่ทรัพย์สินของตนเองหรือครอบครัวทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถนั้นก่อน

2.1.4 เจ้าของข้อมูลส่วนบุคคลที่เป็นคน “ไร้ความสามารถ” หมายถึง บุคคลที่ศาลสั่งให้เป็น คนไร้ความสามารถ เช่น เป็นบุคคลวิกลจริต ทั้งนี้ ในการให้ความยินยอมใด ๆ จะต้องได้รับความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถนั้นก่อน

2.2 ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นผู้ประกอบการที่ทำธุรกิจในนามบุคคลธรรมดา หรือทำในรูปแบบบริษัท และไม่ว่าจะเป็นบริษัทเล็กหรือบริษัทใหญ่ ประกอบกิจการเป็นบริษัทจำกัด หรือ บริษัทมหาชนจำกัด และไม่ได้จำกัดแต่เฉพาะในภาคธุรกิจเท่านั้น หน่วยงานของรัฐก็เช่นกัน หากเขาเหล่านั้น มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เขามีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล”

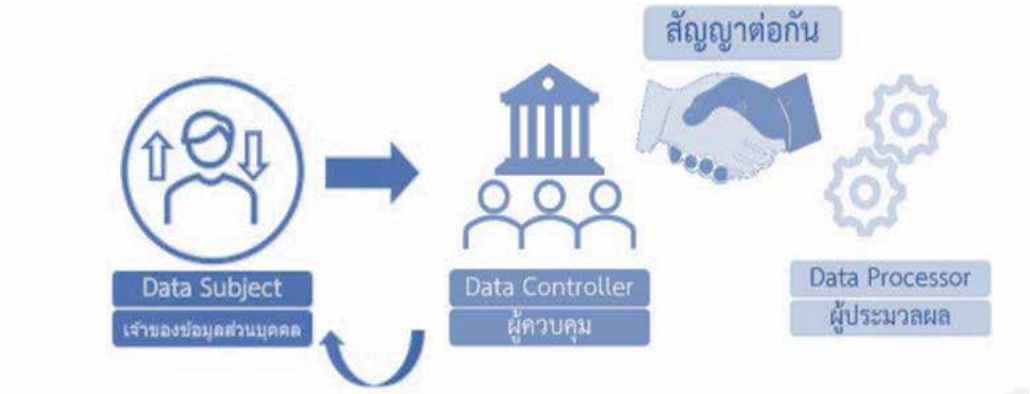
หน้าที่ของผู้ควบคุมข้อมูล มีดังนี้

หน้าที่	รายละเอียด
1. เก็บรวบรวม ใช้ เปิดเผย ให้เป็นไปตามกฎหมาย	การเก็บรวบรวม ใช้ เปิดเผย ต้องมีฐานทางกฎหมายรองรับ และต้องดำเนินการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ไม่ว่าจะเก็บรวบรวมข้อมูลมาจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เข้าข้อยกเว้น ซึ่งเกี่ยวข้องกับหน้าที่ในการจัดเตรียมเอกสารต่าง ๆ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมั่นใจว่า หากยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลเข้าไปเก็บรวบรวมข้อมูลของเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลจะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอย่างไร ตัวอย่างเช่น บริษัทมีหน้าที่ต้องจัดเก็บรวบรวมข้อมูลลูกจ้าง ได้แก่ ชื่อ นามสกุล วันที่เริ่มจ้าง อัตราค่าจ้าง เพื่อจัดทำทะเบียนลูกจ้าง ตามกฎหมายคุ้มครองแรงงาน เป็นต้น
2. เปิดช่องให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามกฎหมาย	บันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เมื่อผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมระบุเหตุผลในรายการบันทึกรายการตามมาตรา 39 ตัวอย่างเช่น พนักงานของบริษัทขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคล แต่การเข้าถึงดังกล่าวนั้นไปกระทบสิทธิของบุคคลอื่น เช่นนี้บริษัทมีสิทธิในการปฏิเสธได้ และต้องมีการบันทึกเหตุแห่งการปฏิเสธไว้
3. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล	เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม และเป็นไปตามมาตรฐานขั้นต่ำ ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของลูกจ้างในบริษัทว่าในกิจกรรมนั้นๆ ว่าฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสาร หรือมีการล็อคกุญแจหรือไม่
4. จัดให้มีมาตรการป้องการไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ	ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น มีการโอนข้อมูลส่วนบุคคลให้ผู้ประมวลผล ต้องมีการดำเนินการเพื่อไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจ หรือโดยไม่ถูกต้องตามกฎหมาย

หน้าที่	รายละเอียด
5. จัดให้มีระบบตรวจสอบเพื่อดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้	จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย การยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ตัวอย่างเช่น ข้อมูลทะเบียนลูกจ้าง ควรมีการจัดเก็บอย่างน้อย 2 ปี และควรมีการทำลายเมื่อหมดความจำเป็นในการจัดเก็บ หรือในกรณีที่มีข้อพิพาทระหว่างนายจ้าง หรือลูกจ้าง บริษัทอาจสามารถเก็บได้ถึง 10 ปี ตามอายุความ กฎหมายแพ่งและพาณิชย์
6. แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล	ต้องแจ้งเหตุละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับแต่เมื่อทราบเหตุดังกล่าว เท่าที่จะสามารถกระทำได้ ทั้งนี้ ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า
7. แต่งตั้งตัวแทนในราชอาณาจักร	หากผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกประเทศไทย ผู้ควบคุมส่วนบุคคลต้องแต่งตั้งตัวแทนของตนในประเทศไทย โดยต้องแต่งตั้งเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในประเทศไทยและได้รับมอบอำนาจให้กระทำแทนโดยไม่มีข้อจำกัดความรับผิดใดๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของผู้ควบคุมข้อมูล
8. หน้าที่ในการจัดทำบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities : RoPA)	ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้
9. จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)	การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม PDPA
10. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)	หากเข้าหลักเกณฑ์ที่กฎหมายกำหนดให้ต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยจะต้องแจ้งข้อมูลเกี่ยวกับ DPO สถานที่ติดต่อ และข้อมูลการติดต่ออื่น ๆ ให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ

2.3 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล หรือ Data Processor คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่ง หรือ ในนามหรือภายใต้คำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ไม่ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล



ภาพความสัมพันธ์ 3 ฝ่าย

เมื่อเจ้าของข้อมูลส่วนบุคคล ได้มอบความไว้วางใจและให้ข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลในการเก็บรวบรวใช้และเปิดเผยข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะต้องมีความรอบคอบในการเก็บรักษาข้อมูล ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลทำข้อมูลรั่วไหล บุคคลคนแรกที่จะต้องรับผิดชอบ คือ ผู้ควบคุมส่วนบุคคล ดังนั้น จึงจะต้องมีการทำสัญญาร่วมกันเพื่อกำหนดมาตรฐานในการดำเนินการภายใต้ PDPA ให้เกิดความรับผิดชอบร่วมกัน และจำเป็นจะต้องสร้างความเข้าใจร่วมกัน ดังนี้

2.3.1 พนักงานในหน่วยงาน องค์กร หรือ สถาบัน ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller พนักงานและ ลูกจ้าง ทุกระดับ ไม่ว่าจะเป็นเจ้าหน้าที่ ผู้จัดการ หรือ ผู้บริหารแม้จะมีอำนาจตัดสินใจก็เป็นเพียงตัวแทน หรือ ผู้แทนที่กระทำการในนามของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

2.3.2 พนักงานในหน่วยงาน องค์กร หรือ สถาบัน ไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล หรือ Data Processor พนักงานของนิติบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่กระทำตามคำสั่งหรือในนามของนิติบุคคลนั้นไม่ใช่ผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล มีดังนี้

หน้าที่	รายละเอียด
1. ประมวลผลข้อมูลส่วนบุคคลภายใต้คำสั่งผู้ควบคุมข้อมูลส่วนบุคคล	ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น บริษัทมีการจ้างบริษัทภายนอก เพื่อดำเนินการด้านเงินเดือนให้กับลูกจ้างภายในบริษัท บริษัทที่รับประมวลผลข้อมูลส่วนบุคคลดังกล่าวต้องทำตามคำสั่ง หากทำนอกคำสั่ง ผู้ประมวลผลจะกลายเป็นผู้ควบคุมข้อมูลในกิจกรรมที่ทำนอกคำสั่งนั้น

หน้าที่	รายละเอียด
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ตัวอย่างเช่น ต้องมีการกำหนดการเข้าถึงข้อมูลของลูกจ้างในบริษัทว่าในกิจกรรมนั้นๆ ฝ่ายใดมีสิทธิในการเข้าถึงบ้าง มีระดับการเข้าถึงอย่างไร หรือในกรณีที่มีการเก็บในรูปแบบเอกสาร Hard copy มีการเก็บเข้าแฟ้ม ตู้เอกสารหรือมีการล็อคกุญแจหรือไม่
3. จัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล	จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรม การประกาศกำหนด
4. ทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล	การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม PDPA

2.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

ตามมาตรา 41 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มี เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่ คณะกรรมการประกาศกำหนด

2. การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

3. กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวข้อมูลส่วนบุคคลประเภทอ่อนไหวตามมาตรา 26

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการ หรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามที่คณะกรรมการประกาศกำหนด ตามมาตรา 29 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าว ต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย และในส่วนของการกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น อยู่ในขั้นตอนของการจัดทำกฎหมายลำดับรอง โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

คุณสมบัติและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล นั้นจะเป็นพนักงาน ผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล โดยอาจจะเป็นคนเดียวหรือคณะทำงานก็ได้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีสิทธิเข้าถึงข้อมูลส่วนบุคคลและรายละเอียดการประมวลผลข้อมูลส่วนบุคคลภายในองค์กรโดยได้รับการสนับสนุนที่เพียงพอด้านอุปกรณ์ เครื่องมือ งบประมาณ และอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคล และได้รับความคุ้มครองจากการถูกเลิกจ้างด้วยเหตุที่ปฏิบัติหน้าที่ตาม PDPA รวมถึงต้องสามารถรายงานถึงผู้บริหารสูงสุดขององค์กรได้โดยตรง

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีดังนี้

หน้าที่	รายละเอียด
1. ให้คำแนะนำ	ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
2. ตรวจสอบการดำเนินการ	ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตาม PDPA
3.ประสานงานและให้ความร่วมมือกับสำนักงาน	ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4.รักษาความลับของข้อมูล	รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มา เนื่องจากการปฏิบัติหน้าที่

บทที่ 3

หลักการคุ้มครองข้อมูลส่วนบุคคลกับการคุ้มครองแรงงาน

1. หลัก 7 ประการ การคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองแรงงาน มีดังนี้

หลักการที่ 1 : ถูกกฎหมาย เป็นธรรม และ โปร่งใส (Lawfulness Fairness and Transparency)

การประมวลผลข้อมูลส่วนบุคคลจะมีขึ้นได้เฉพาะกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นมีเหตุผลความจำเป็นที่สามารถอ้างอิงฐานการประมวลผลทางกฎหมาย (Lawful Basis) ที่กฎหมายรับรอง โดยจะต้องมีการประกาศและแสดงต่อลูกจ้างทราบถึงเหตุผลความจำเป็นและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลอย่างเปิดเผย และง่ายต่อการทำความเข้าใจเพื่อให้ลูกจ้างสามารถตัดสินใจต่อการประมวลผลข้อมูลที่อาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้ ตัวอย่างเช่น การเก็บข้อมูลทะเบียนลูกจ้าง สามารถใช้ฐาน การปฏิบัติตามกฎหมาย 24(6) (Legal obligation) ในการจัดเก็บข้อมูลของลูกจ้างได้

หลักการที่ 2 : จำกัดวัตถุประสงค์ (Purpose Limitation)

การประมวลผลข้อมูลส่วนบุคคลสามารถกระทำได้อย่างจำกัดเท่าที่จำเป็นภายใต้ขอบเขตวัตถุประสงค์ที่แจ้งไว้กับลูกค้า เพื่อให้การประมวลผลข้อมูลส่วนบุคคลสอดคล้องตามหลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใสอย่างแท้จริง เว้นแต่กรณีที่มีวัตถุประสงค์ใหม่และวัตถุประสงค์นั้นเกี่ยวข้องหรือสอดคล้องกับวัตถุประสงค์เดิม ตัวอย่างเช่น การเก็บข้อมูลสุขภาพของลูกจ้าง เพื่อใช้ในการดำเนินการเป็นเอกสารอ้างอิงประกอบการลาป่วย เมื่อป่วยเกิน 3 วัน ตามกฎหมายคุ้มครองแรงงาน นายจ้างหรือบริษัท ไม่สามารถนำข้อมูลดังกล่าวไปใช้นอกวัตถุประสงค์นอกเหนือจากการใช้เป็นเอกสารประกอบการลาได้ เว้นแต่ได้รับความยินยอมจากลูกจ้าง

หลักการที่ 3 : การใช้ข้อมูลอย่างจำกัด (Data Minimization)

การประมวลผล เก็บรวบรวม ใช้ เปิดเผย และ ระยะเวลาเก็บข้อมูล ควรดำเนินการเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายตามมาตรา 22 และควรพิจารณาอย่างรอบคอบ ตัวอย่างเช่น การจัดเก็บสำเนาบัตรประชาชน ซึ่งมีข้อมูลศาสนาซึ่งเป็นข้อมูลอ่อนไหวตามมาตรา 26 นายจ้างต้องพิจารณาว่าการเก็บข้อมูลศาสนาดังกล่าว นายจ้างมีความจำเป็นต้องเก็บหรือไม่ เพราะถ้าหากไม่มีความจำเป็นในการเก็บแล้ว ควรมีมาตรการ เช่น การถมดำ หรือ การขีดฆ่าข้อมูลศาสนา เพื่อเป็นการลดภาระและปัญหาที่ตามมากการเก็บข้อมูลอ่อนไหว

หลักการที่ 4 : ความถูกต้องของข้อมูล (Data Accuracy)

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller จะต้องดำเนินการเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบ หรือแก้ไขโดยไม่ชักช้า และควรมีการจัดช่องทางการติดต่อที่ง่าย สะดวก รวดเร็วในการขอใช้สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องสมบูรณ์และทันสมัยด้วย

หลักการที่ 5 : การจำกัดการจัดเก็บข้อมูล (Storage Limitation)

ข้อมูลส่วนบุคคลจะต้องเก็บในระยะเวลาที่เหมาะสม เพื่อให้เป็นไปวัตถุประสงค์ในการประมวลผลข้อมูล หรือตามกฎหมายอื่น ๆ ตัวอย่างเช่น ในกิจกรรมการจัดทำทะเบียนลูกจ้าง ตามพระราชบัญญัติคุ้มครองแรงงาน มาตรา 115 ได้

มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้จัดเก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดกาจ้างแต่ละราย จะเห็นได้ชัดว่า การกำหนดระยะเวลาการทำลายข้อมูลดังกล่าวตามกฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดรายละเอียดการทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการดำเนินการลบ หรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว

หลักการที่ 6 : การธำรงไว้ซึ่งความลับและความสมบูรณ์ของข้อมูล (Integrity and Confidentiality)

ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมนั้นจะต้องมีความสมบูรณ์ ไม่ผิดเพี้ยนหรือเกิดเหตุที่ทำให้ข้อมูลขาดหายลบเลือนจากการจัดเก็บ มีการเก็บข้อมูลส่วนบุคคลอย่างเป็นความลับ บุคคลอื่นที่ไม่เกี่ยวข้องต้องไม่สามารถเข้าถึงข้อมูลได้โดยไม่มีสิทธิ รวมทั้งข้อมูลต้องมีความพร้อมใช้งาน กล่าวคือ แม้เกิดสภาวะใดที่ทำให้ไม่สามารถใช้งานข้อมูลส่วนบุคคลนั้นได้ชั่วคราว เช่น ไฟดับ ติดไวรัส ถูกเข้ารหัส ถูกขโมยอุปกรณ์บันทึกข้อมูล เป็นต้น ก็ต้องมีมาตรการที่ทำให้ข้อมูลส่วนบุคคลที่มีการจัดเก็บยังสามารถนำมาใช้งานได้เสมือนหนึ่งว่าไม่ได้เกิดเหตุการณ์ดังกล่าว

หลักการที่ 7 : ความรับผิดชอบ (Accountability)

ความรับผิดชอบทางกฎหมายตามมาตรา 81 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ บุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือ ในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และ ละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

2. ฐานทางกฎหมาย มาตรา 24 ในการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการคุ้มครองแรงงาน มี 7 ฐาน ดังต่อไปนี้

1. ฐานความยินยอม (มาตรา 19 และ มาตรา 24)

มาตรา 19 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล

2) การขอความยินยอมต้องทำโดยชัดแจ้ง

3) แจ้งวัตถุประสงค์อย่างชัดเจน

4) ต้องไม่เป็นส่วนหนึ่งของสัญญา

5) เข้าถึงได้ง่าย เข้าใจง่าย

6) การให้ความยินยอมต้องมีความอิสระ

7) ต้องถอดถอนง่ายและจะถอนความยินยอมเมื่อใดก็ได้ โดยบทเฉพาะกาล มาตรา 95 ผู้ควบคุมข้อมูลสามารถเก็บและใช้ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนที่ PDPA จะมีผลบังคับใช้นั้นต่อไปได้ตามวัตถุประสงค์เดิมและต้องกำหนดวิธีการยกเลิกความยินยอมและประชาสัมพันธ์ให้เจ้าของข้อมูลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคล เก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลดังกล่าวจะต้องสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย เช่น ผ่านเว็บไซต์ แต่มีข้อควรระวังในบริษัทในเรื่องของความสัมพันธ์ระหว่าง นายจ้างและลูกจ้างเพราะเป็นความสัมพันธ์ที่ไม่เท่าเทียมกันอาจเกิดความไม่เป็นอิสระ

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง

2) ผู้เยาว์อายุ 10 – 20 ปี อาจให้ความยินยอมโดยลำพัง หรือจาก ผู้ใช้อำนาจปกครองผู้เยาว์ด้วย แล้วแต่กรณี

3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์

4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

2. ฐานปฏิบัติตามสัญญา

ฐานสัญญาถือเป็นฐานที่จำเป็นเพื่อการปฏิบัติตามสัญญาและใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา เช่น การขอสินเชื่อเพื่อเปิดบัญชีเงินฝาก การให้สินเชื่อ การทวงถามหนี้สินที่ต้องประมวลข้อมูลการเงิน โดยฐานปฏิบัติตามสัญญา จำเป็นเพื่อปฏิบัติตามสัญญาโดยตรงทั้งก่อนและขณะเข้าทำสัญญาทางการค้าแม้ไม่ได้ระบุเป็นเงื่อนไขในสัญญา เฉพาะข้อมูลส่วนบุคคลทั่วไปของเจ้าของข้อมูลคู่สัญญาเท่านั้นเมื่อเข้าฐานปฏิบัติตามสัญญาก็ไม่ต้องขอความยินยอมเพิ่มเติม และเมื่อไม่ใช่ฐานความยินยอม จึงไม่อาจถอนความยินยอมได้

3. ฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ในฐานนี้มี “ความจำเป็น” ตามกฎหมาย ไม่ใช่ทางเลือกเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล แต่เป็นหน้าที่ตามบทบัญญัติแห่งกฎหมายที่ต้องปฏิบัติตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ

ตัวอย่าง พ.ร.บ.คุ้มครองแรงงาน บริษัท มีหน้าที่ยื่นภาษีให้กรมสรรพากรและกรมฯ อาจขอให้บริษัทเปิดเผยข้อมูลตามบทบัญญัติแห่งประมวลรัษฎากรหมวด 3 มาตรา 76 นายจ้างจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลโดยอาศัย ชื่อ สกุล เลขที่บัตรประชาชน เลขที่ผู้เสียภาษี ตามมาตรา 113 (ทะเบียนลูกจ้าง) ดังนั้นนายจ้างเก็บรวบรวม ข้อมูลส่วนบุคคล ชื่อ สกุล สัญชาติ เพศ วันเดือนปีเกิด ที่อยู่ เงินเดือน ตำแหน่ง วันที่เริ่มจ้าง และวันที่สิ้นสุดการจ้างงาน เพื่อจัดทำทะเบียนลูกจ้างได้ตามกฎหมาย

4. ฐานผลประโยชน์สาธารณะ อำนาจรัฐ

ผู้ประมวลผลข้อมูลตามฐานนี้มักเป็นเจ้าหน้าที่ หรือ องค์กรของรัฐ ที่ปฏิบัติภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชนหากการประมวลผลข้อมูลนั้นมีความจำเป็นตามอำนาจของรัฐหรือเป็นไปเพื่อ ประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมายของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง เช่น กรมสรรพากรคำนวณข้อมูลเงินเดือนลูกจ้างเพื่อตรวจสอบรายการที่ยื่นภาษี

5. ฐานผลประโยชน์อันชอบธรรมด้วยกฎหมาย

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ฐานนี้ในกรณีที่จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล และเป็นไปอย่างสมเหตุสมผล เช่น การตรวจสอบอาชญากรรมและการฉ้อโกง อันส่งผลต่อหน่วยงานหรือเป็นการช่วยเหลือเจ้าหน้าที่รัฐตามกฎหมาย ในฐานนี้ตามกฎหมายมาตรา 24 มีหลัก 3 ข้อ

(1) จะต้องอยู่ในความคาดหมายของเจ้าของข้อมูล

(2) มีความเสี่ยงต่อการกระทบสิทธิเสรีภาพของเจ้าของข้อมูลในระดับต่ำ

(3) มีความชอบธรรม (สำคัญ)

6. ฐานระงับอันตรายต่อชีวิต สุขภาพ ร่างกายของบุคคล

ฐานระงับอันตรายต่อชีวิต สุขภาพ ร่างกายของบุคคล กรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อน หรือ sensitive data เช่น หมู่เลือด ข้อมูลสุขภาพ สามารถใช้ได้กรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เช่น เจ้าของข้อมูลส่วนบุคคลเกิดอุบัติเหตุ แต่หากขอความยินยอมได้ควรขอก่อน ตามมาตรา 24 เป็น ข้อมูลทั่วไป และมาตรา 26 เป็นข้อมูลละเอียดอ่อน

7. ฐานการจัดทำเอกสารประวัติศาสตร์-วิจัย-สถิติ

ในฐานจดหมายเหตุ วิจัย สถิติ นี้ไม่มีใน GDPR แต่อย่างไรก็ตามควรเป็นไปตามมาตรฐานการวิจัย เป็นการเก็บรวบรวม จัดเก็บข้อมูลเพื่อการจัดทำเอกสารทางประวัติศาสตร์ หรืองานวิจัย หรืองานสถิติ ซึ่งจะต้องมีการระบุชัดเจน

3. ฐานทางกฎหมาย มาตรา 26 ในการประมวลผลข้อมูลส่วนบุคคลละเอียดอ่อนกับการคุ้มครองแรงงาน มี 6 ฐาน ดังต่อไปนี้

1. ฐานความยินยอม (มาตรา 19 และ มาตรา 26)

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจาก เจ้าของข้อมูลส่วนบุคคล

1) การขอความยินยอมจากเจ้าของข้อมูลจะต้องขอก่อนหรือในขณะที่ประมวลผลข้อมูลส่วนบุคคล

2) การขอความยินยอมต้องทำโดยชัดแจ้ง

3) แจ้งวัตถุประสงค์อย่างชัดเจน

4) ต้องไม่เป็นส่วนหนึ่งของสัญญา

5) เข้าถึงได้ง่าย เข้าใจง่าย

6) การให้ความยินยอมต้องมีความอิสระ

7) ต้องถอดถอนง่ายและจะถอนความยินยอมเมื่อใดก็ได้ โดยบทเฉพาะกาล มาตรา 95 ควบคุมข้อมูลสามารถเก็บและใช้ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนที่ PDPA จะมีผลบังคับใช้นั้นต่อไปได้ตามวัตถุประสงค์เดิม และต้องกำหนดวิธีการยกเลิกความยินยอมและประชาสัมพันธ์ให้เจ้าของข้อมูลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วน บุคคลดังกล่าวจะต้องสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย เช่น ผ่านเว็บไซต์ แต่มีข้อควรระวัง ในบริษัทในเรื่องของความสัมพันธ์ระหว่าง นายจ้างและลูกจ้างเพราะเป็นความสัมพันธ์ที่ไม่เท่าเทียมกัน อาจเกิดความไม่เป็นอิสระ ตัวอย่าง กรณีที่ความยินยอมในการประมวลเป็นประโยชน์แก่ลูกจ้าง เช่น บริษัทมอบผลประโยชน์บางอย่างแก่สมาชิกในครอบครัว

มาตรา 20 การขอความยินยอมกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นบุคคลหย่อนความสามารถ

1) ผู้เยาว์อายุไม่เกิน 10 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครอง

2) ผู้เยาว์อายุ 10 – 20 ปี ให้ขอความยินยอมจาก ผู้ใช้อำนาจปกครองผู้เยาว์ด้วย แล้วแต่กรณี

3) คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้พิทักษ์

4) คนไร้ความสามารถ ให้ขอความยินยอมจาก ผู้อนุบาล

มาตรา 26 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่.....

2. ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ฐานระงับอันตรายต่อร่างกายสุขภาพและชีวิตกรณีที่มีเหตุจำเป็นต้องใช้ข้อมูลละเอียดอ่อนหรือ sensitive data เช่น กรุ๊ปเลือด ข้อมูลสุขภาพ สามารถใช้ได้กรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เช่น เจ้าของข้อมูลส่วนบุคคลเกิดอุบัติเหตุ แต่หากขอความยินยอมได้ควรขอก่อน ตามมาตรา 24 เป็น ข้อมูลทั่วไป และมาตรา 26 เป็นข้อมูลละเอียดอ่อน

3. ฐานการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา สหภาพแรงงาน โดยต้องไม่เปิดเผยไปสู่บุคคลภายนอก

4. ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

5. จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

6. จำเป็นต้องปฏิบัติตามกฎหมาย เฉพาะที่เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการใช้บริการด้านสังคมสงเคราะห์ ประโยชน์สาธารณะด้านสาธารณสุข การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นที่สำคัญ

4. สิทธิของเจ้าของข้อมูล

สิทธิของเจ้าของข้อมูลส่วนบุคคล มี 9 ข้อ ดังนี้

1. สิทธิในการถอนความยินยอม ตามมาตรา 19 วรรค 5 กำหนดไว้ดังนี้

1) การถอนความยินยอมจะต้องถอนเมื่อใดก็ได้

2) ต้องถอนได้โดยวิธีที่ง่ายเหมือนเมื่อตอนให้ความยินยอม

3) การถอนต้องไม่มีผลย้อนหลังและไม่ส่งผลต่อการประมวลผลที่ยินยอมไปแล้ว

4) ถ้าข้อมูลติดฐานอื่น เช่น ฐานสัญญา ฐานปฏิบัติตามกฎหมายจะไม่สามารถถอนความยินยอมได้

นายจ้างต้องแจ้งลูกจ้างหากลูกจ้างได้ให้ความยินยอมให้บริษัทเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (ไม่ว่าจะเป็นความยินยอมที่ลูกจ้างให้ไว้ก่อนวันที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับหรือหลังจากนั้น) ลูกจ้างมีสิทธิที่จะถอนความยินยอมเมื่อใดก็ได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลอยู่กับนายจ้าง เว้นแต่มีข้อจำกัดสิทธินั้นโดยกฎหมายหรือมีสัญญาที่ให้ประโยชน์อยู่

ทั้งนี้ นายจ้างควรแจ้งรายละเอียดว่า การถอนความยินยอมอาจส่งผลกระทบต่อการใช้ผลิตภัณฑ์ และ/หรือบริการต่างๆ เช่น จะไม่ได้รับสิทธิประโยชน์ โปรโมชันหรือข้อเสนอใหม่ ๆ ไม่ได้รับผลิตภัณฑ์หรือบริการที่ดียิ่งขึ้นและสอดคล้องกับความต้องการ หรือไม่ได้รับข้อมูลข่าวสารอันเป็นประโยชน์

2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล สิทธิขอเข้าถึงข้อมูลส่วนบุคคล ตามมาตรา 30 มีดังนี้

1) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูล ที่เกี่ยวกับตน หรือ ขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ไม่ได้ให้ความยินยอม

2) ต้องทำตามคำขอโดยไม่ชักช้าไม่เกินระยะเวลา 30 วันนับแต่วันที่ได้รับคำขอ

3) สามารถปฏิเสธได้หากเป็นไปตามกฎหมายหรือคำสั่งศาล

4) หากสามารถปฏิเสธได้ ต้องบันทึกการปฏิเสธคำขอพร้อมเหตุผลไว้ในรายการ มาตรา 39

ลูกจ้างมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน และขอให้นายจ้างทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้ รวมถึงขอให้นายจ้างเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัท ทั้งนี้ นายจ้างอาจปฏิเสธคำขอหากการเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อสิทธิ และเสรีภาพของบุคคลอื่น หรือนายจ้างต้องปฏิบัติตามกฎหมาย หรือคำสั่งศาลที่ห้ามเปิดเผยข้อมูลส่วนบุคคลนั้น

3. สิทธิในการได้รับแจ้ง ลูกจ้างมีสิทธิในการที่จะได้ทราบถึงรายละเอียดเกี่ยวกับการใช้ข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคลหรือเหตุการณ์ต่างๆ โดยต้องทำการแจ้งก่อน หรือขณะที่การประมวลผลข้อมูลส่วนบุคคลนั้นจะเริ่มมีขึ้น เพื่อลูกจ้างสามารถตัดสินใจเกี่ยวกับข้อมูลอันอาจกระทบต่อสิทธิความเป็นส่วนตัวของตนได้ ในแง่นี้ สิทธิดังกล่าวจึงเรียกร้องให้นายจ้างจัดให้มีการแจ้งด้วยการสื่อสารที่ชัดเจนและเข้าใจง่าย โดยลูกจ้างต้องได้รับการแจ้งให้ทราบรายละเอียดก่อนหรือขณะเก็บข้อมูล ตามมาตรา 23 ดังนี้

1) วัตถุประสงค์ในการเก็บและฐานทางกฎหมาย

2) กรณีต้องใช้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือตามสัญญา และผลกระทบหากไม่ให้ข้อมูล

3) การเก็บขอมูลนั้นเป็นการเก็บข้อมูลอะไร เก็บนานเท่าไหร่

4) จะมีการเปิดเผยข้อมูลให้หน่วยงานหรือบุคคลใดบ้าง

5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ วิธีการติดต่อ รวมถึงรายละเอียดของผู้เป็น DPO (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

4. สิทธิในการโอนย้ายข้อมูล เจ้าของข้อมูลมีสิทธิขอรับข้อมูลจากผู้ควบคุมข้อมูล ถ้าข้อมูลอยู่ในรูปแบบที่สามารถอ่านได้และใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลได้ด้วยวิธีการอัตโนมัติ ตามมาตรา 31 สามารถทำได้ดังนี้

1) ขอให้ส่งข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น

2) ขอรับข้อมูลที่ส่งหรือโอนไปให้ผู้ควบคุมข้อมูลอื่นแต่จะใช้ได้เฉพาะฐานยินยอมและฐานสัญญา หรือฐานอื่นใดตามที่คณะกรรมการประกาศกำหนด แต่จะใช้ไม่ได้กับฐานปฏิบัติหน้าที่ตามกฎหมายหรือการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะและหากเป็นการกระทบกระเทือนสิทธิ เสรีภาพผู้อื่น มีสิทธิปฏิเสธคำขอและต้องบันทึกเหตุผลไว้ในรายการตามมาตรา 39

นายจ้างมีสิทธิขอรับข้อมูลส่วนบุคคลของลูกจ้าง ในกรณีที่บริษัทได้จัดทำข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบให้สามารถอ่านหรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ และสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิขอให้นายจ้างส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ และมีสิทธิขอรับข้อมูลส่วนบุคคลที่บริษัทส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่ไม่สามารถดำเนินการได้เพราะเหตุทางเทคนิค

ทั้งนี้ ข้อมูลส่วนบุคคลของลูกจ้างข้างต้นต้องเป็นข้อมูลส่วนบุคคลที่ลูกจ้างได้ให้ความยินยอมแก่นายจ้างในการเก็บรวบรวม ใช้ และ/หรือเปิดเผย หรือเป็นข้อมูลส่วนบุคคลที่นายจ้างจำเป็นต้องเก็บรวบรวม ใช้ และ/หรือเปิดเผยเพื่อให้ลูกจ้างสามารถใช้ผลิตภัณฑ์และ/หรือบริการของบริษัทได้ตามความประสงค์ซึ่งลูกจ้างเป็นคู่สัญญาอยู่กับบริษัท หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนใช้ผลิตภัณฑ์และ/หรือบริการ หรือเป็นข้อมูลส่วนบุคคลอื่นตามที่ผู้มีอำนาจตามกฎหมายกำหนด

5. สิทธิคัดค้านการให้ใช้ข้อมูล

ลูกจ้างมีสิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในเวลาใดก็ได้ หากการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำขึ้นเพื่อการดำเนินงานที่จำเป็นภายใต้ประโยชน์โดยชอบด้วยกฎหมายของนายจ้าง หรือของบุคคลหรือนิติบุคคลอื่น โดยไม่เกินขอบเขตที่สามารถคาดหมายได้อย่างสมเหตุสมผล หากยื่นคัดค้านและนายจ้างจะยังคงดำเนินการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปเฉพาะที่สามารถแสดงเหตุผลตามกฎหมายได้ว่ามีความสำคัญยิ่งกว่าสิทธิขั้นพื้นฐาน หรือเป็นไปเพื่อการยืนยันสิทธิตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการต่อสู้ในการฟ้องร้องตามกฎหมาย ตามแต่ละกรณี

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เกี่ยวกับตนเมื่อใดก็ได้ ตามมาตรา 32 คัดค้านได้ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม โดยใช้ฐานมาตรา 24 ฐาน Public Interest อันเป็นเพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลมีการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ ฐาน Legitimate Interest ประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล วัตถุประสงค์เพื่อการตลาดแบบตรง หรือเพื่อการศึกษา วิจัย หรือสถิติทางการตลาด ในกรณีที่นายจ้างไม่สามารถปฏิเสธการคัดค้านได้ นายจ้างต้องดำเนินการแยกส่วนข้อมูลฯ นั้นโดยทันทีและห้ามประมวลผลโดยเด็ดขาด

6. สิทธิขอให้ลบข้อมูล สิทธิขอให้ลบข้อมูลและสิทธิที่จะถูกลืม ตามมาตรา 33 เจ้าของข้อมูลมีสิทธิขอให้ลบทำลาย หรือ ทำให้ข้อมูลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ลูกจ้างมีสิทธิขอลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หากเชื่อว่าข้อมูลส่วนบุคคลของท่านถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายที่เกี่ยวข้อง ไม่ได้ขอความยินยอม ไม่มีฐานทางกฎหมายรองรับ เห็นว่านายจ้างหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ที่เกี่ยวข้องในประกาศความเป็นส่วนตัว หรือเมื่อได้ใช้สิทธิขอถอนความยินยอม หรือใช้สิทธิขอคัดค้านตามข้างต้นแล้ว เว้นแต่เป็นกรณีที่ต้องปฏิบัติตามกฎหมาย มีสัญญาผูกพัน หรือมีการใช้สิทธิเรียกร้องตามกฎหมายที่เกี่ยวข้องในการเก็บรักษาข้อมูลดังกล่าว

7. สิทธิขอให้ระงับใช้ข้อมูล

ตามมาตรา 34 เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิขอให้ระงับใช้ข้อมูลได้ชั่วคราว ในกรณีเจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลให้เป็นปัจจุบันหรืออยู่ในระหว่างการตรวจสอบในกรณีต่าง ๆ เช่น ลูกจ้างกำลังย้ายบ้านและกังวลว่าบริษัทจะส่งจดหมายไปตามที่อยู่เก่า ระหว่างกำลังตรวจสอบข้อมูลที่สงสัยว่าได้มาโดยมิชอบหรืออยู่ระหว่างการตรวจสอบการขอใช้สิทธิคัดค้านของลูกจ้าง เป็นต้น หรือกรณีอื่นใดที่บริษัทหมดความจำเป็นและต้องลบหรือทำลายข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้องแต่ลูกจ้างขอให้บริษัทระงับการใช้แทน

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

9. สิทธิในการร้องเรียน เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องเรียนผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลข้อมูลส่วนบุคคลของลูกจ้าง (หรือผู้รับจ้าง) กรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตาม PDPA แล้วทำให้ลูกจ้างได้รับผลกระทบในสิทธิและเสรีภาพได้ ตามมาตรา 73

5. ความรับผิดโทษตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

บทลงโทษความรับผิดตามกฎหมายตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA มีโทษ ดังนี้

โทษอาญา

1) ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) โดยมิชอบหรือนอกเหนือวัตถุประสงค์ ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive data) ไปยังต่างประเทศ

2) หรือที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย มีโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

3) เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

4) ล่วงรู้ข้อมูลเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้แล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบด้วยกฎหมายต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน500,000 บาท หรือ ทั้งจำทั้งปรับ

5) กรรมการหรือผู้จัดการหรือบุคคลใดที่รับผิดชอบในการดำเนินงานของนิติบุคคล หากมีการสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้นด้วย สำหรับโทษทางอาญานี้เป็นโทษที่สามารถยอมความได้

โทษทางปกครอง

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

ความรับผิดทางแพ่ง

ความผิดทางแพ่งตามมาตรา 77 ต้องจ่ายสินไหมทดแทนตามจริง หรือศาลอาจพิจารณาเพื่อเป็นการลงโทษให้จ่ายเพิ่มอีก 2 เท่าได้ หากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลข้อมูลส่วนบุคคล

- จงใจหรือประมาทเลินเล่อ อันเป็นเหตุให้เกิดความเสียหายแก่เจ้าของข้อมูล จะเกิดความผิดทางปกครอง
- การกระทำที่ฝ่าฝืนข้อห้ามตาม พ.รบ. คุ้มครองข้อมูลส่วนบุคคล
- การกระทำที่ไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล สั่งให้กระทำและข้อห้ามมิให้กระทำการ

6. สิ่งที่องค์กรต้องเตรียมตัว

6.1 การสร้างความรับรู้ขององค์กร การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะต้องอาศัยการบริหารจัดการแบบบนลงล่าง (top-down) ซึ่งเป็นการสื่อสารจากผู้บริหารไปยังบุคลากรในองค์กร ขณะเดียวกัน จำเป็นอย่างยิ่งที่องค์กรจะต้องสร้างความรู้ความเข้าใจให้กับบุคลากรระดับปฏิบัติการในการปฏิบัติตามกฎหมายจะต้องอาศัยความมีส่วนร่วมจากทุกหน่วยในองค์กร หากหน่วยหนึ่งหน่วยใดในองค์ไม่มีความตระหนัก ไม่ให้ความร่วมมือ หรือเห็นว่าการปฏิบัติตามกฎหมายนี้เป็นภาระ การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่แม้เกิดขึ้นก็อาจมีช่องว่าง และในท้ายที่สุดย่อมส่งผลกระทบต่อองค์กรในภาพรวม

6.2 วิเคราะห์การทำงาน และค้นหากิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นในองค์กรกิจกรรมนี้เป็นกิจกรรมหนึ่งที่มีความสำคัญ แต่ละส่วนงานจะต้องพยายามแสดงกระบวนการทำงาน วิธีการ เส้นทางการใช้งานข้อมูลออกมาให้ชัดเจนและละเอียดที่สุดเท่าที่จะสามารถกระทำได้ โดยอาจอาศัยการทำแบบสอบถาม และการสัมภาษณ์พูดคุยกับฝ่ายงาน เพื่อจัดทำผังการใช้ข้อมูลขององค์กร (data mapping หรือ data flow) เพื่อใช้วิเคราะห์การไหลเวียนของข้อมูลส่วนบุคคลในแต่ละกิจกรรมตั้งแต่กระบวนการการเก็บรวบรวม ใช้ เปิดเผย เก็บรักษา และทำลายข้อมูลส่วนบุคคล เพื่อให้ทราบถึงความเสี่ยงและจะช่วยให้บริษัทสามารถเห็นภาพของจุดบกพร่องและแก้ไขจุดบกพร่องที่เกี่ยวกับข้อมูลส่วนบุคคลได้ในอนาคต

ในส่วนของแบบสอบถาม จะมุ่งเน้นการสร้างกระบวนการทบทวนการใช้งานข้อมูลในองค์กร (data life cycle) ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผย จัดเก็บและสู่ขั้นตอนการลบหรือทำลายข้อมูลส่วนบุคคล โดยในแบบสอบถามองค์กรอาจพิจารณารายการที่กฎหมายกำหนดในเรื่องบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (ม.39) ไม่ว่าจะเป็นการรักษาความปลอดภัยข้อมูล การกำหนดสิทธิการเข้าถึงข้อมูล (access control) ระยะเวลาการลบทำลายข้อมูล ความจำเป็นของข้อมูล วิธีการในการเปิดเผยส่งต่อข้อมูล การประเมินความเสี่ยงและผลกระทบเกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

6.3. วิเคราะห์ช่องว่างทางปฏิบัติไม่สอดคล้องตามเงื่อนไขที่กฎหมายกำหนด (Gap analysis) และการจัดแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม

ในขั้นตอนนี้เป็นขั้นตอนที่องค์กรจะมุ่งทำการวิเคราะห์ถึงรายการที่กฎหมายกำหนดให้องค์กร ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการหรือมีการจัดการตามหลักการกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญโดยประเด็นที่เป็นโจทย์สำคัญในการพิจารณาช่องว่างการปฏิบัติตามกฎหมายจะเป็นการพิจารณากับประเด็นดังนี้ ในกรณีที่กฎหมายกำหนดให้มีการตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) องค์กรมีการจัดตั้งและมีการดำเนินการตามหน้าที่ที่กฎหมายกำหนดหรือไม่

1) องค์กรมีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หรือไม่

2) องค์กรมีประกาศความเป็นส่วนตัว (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 Rights Request) หรือไม่

9) กรณีที่องค์กรมีการประมวลผลข้อมูลส่วนบุคคลร่วมกับบุคคลที่สาม โดยเฉพาะอย่างยิ่งกรณีที่เป็นการใช้งานผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรได้จัดให้มีข้อตกลงสัญญา หรือมาตรการคัดเลือกบุคคลที่สามหรือไม่

10) องค์กรมีแนวทางในการเก็บรักษาข้อมูล และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เพียงพอเหมาะสมหรือไม่

11) องค์กรได้จัดให้มีระบบรองรับการทำงานที่เกี่ยวข้องกรณีเกิดเหตุละเมิดต่อข้อมูลส่วนบุคคลแล้วหรือไม่

การจัดแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม

เพื่อให้องค์กรพิจารณาตามเห็นสมควร โดยองค์กรจะพิจารณาเลือกใช้มาตรการมากน้อยเพียงใดนั้น โดยหลักมักขึ้นอยู่กับชั้นการจัดกลุ่มชั้นความลับของข้อมูล (data classification) ความเสี่ยง รวมทั้งความสามารถในด้านงบประมาณขององค์กรสำหรับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่องค์กรจะนำมาปรับใช้ อาจพิจารณาแบ่งออกเป็นมาตรการรักษาความมั่นคงปลอดภัยพื้นฐานทั่วไป เช่น การจัดการสิทธิการเข้าถึง การกำหนดนโยบายการใช้งานอุปกรณ์ส่วนตัว ตลอดจนมาตรการทางเทคนิค อาทิ การจัดการชั้นความลับ การเข้ารหัสข้อมูล การแฝงข้อมูล นอกจากนี้ มาตรการรักษาความปลอดภัยยังรวมไปถึงระบบที่เกี่ยวข้องกับการตรวจสอบติดตาม และการจัดการกรณีเกิดเหตุละเมิดของข้อมูลส่วนบุคคล (data breach)

ในกรณีที่องค์กรไม่สามารถจัดให้มีระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม ไม่ว่าด้วยเหตุผลข้อจำกัดด้านงบประมาณ หรือเหตุผลด้านสัญญาที่องค์กรได้มีการลงทุนระบบที่มีอยู่เดิมไปก่อนหน้า องค์กรควรพิจารณาความจำเป็นในการใช้งานข้อมูลส่วนบุคคลอย่างรอบคอบ โดยอาจยกเลิกกิจกรรมประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นในบางลักษณะ หากองค์กรยังเห็นว่ากิจกรรมประมวลผลดังกล่าวจำเป็นต้องดำเนินต่อไป องค์กรควรจัดให้มีแผนในการเตรียมความพร้อมด้านงบประมาณ หรือแผนการจัดหาผู้ให้บริการที่เหมาะสม และในระหว่างการดำเนินการดังกล่าว องค์กรควรจะคำนึงถึงการประมวลผลข้อมูลด้วยความระมัดระวัง และอาศัยการบริหารจัดการปฏิบัติงานของบุคลากรเพื่อปิดช่องว่าง หรือลดความเสี่ยงที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรแทน

การสร้างองค์ความรู้และความเข้าใจให้กับบุคลากรในองค์กรและการติดตามผลการปฏิบัติงาน

ส่งเสริมให้บุคลากรขององค์กรในระดับปฏิบัติการเกิดความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคลตลอดจนแนวทางหรือวิธีการปฏิบัติงานที่เปลี่ยนแปลงไปอันเนื่องมาจากการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งควรมีการตรวจสอบหรือทำให้แน่ใจว่าบุคลากรในองค์กรมีความตระหนักรู้และเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอที่จะปฏิบัติตามขั้นตอน ข้อกฎหมาย หรือนโยบายคุ้มครองข้อมูลส่วนบุคคลที่บริษัทกำหนดได้อย่างเหมาะสม สำหรับวัตถุประสงค์สำคัญของการเตรียมการเรื่องนี้คือ การทำให้การคุ้มครองข้อมูลส่วนบุคคลเป็นวัฒนธรรมองค์กรและเป็นส่วนหนึ่งของแนวทางการทำงานขององค์กร

การติดตามผลการปฏิบัติตามกฎหมาย (compliance result monitoring) โดยหลังจากที่ได้จัดการองค์กร และเตรียมความพร้อมในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วเสร็จ จำเป็นอย่างยิ่งที่องค์กรจะต้องจัดให้มีแนวทางในการติดตามการทำงานเป็นระยะ และเป็นประจำอย่างต่อเนื่อง ตั้งแต่ในกระบวนการเก็บบันทึก กระบวนการรักษาความมั่นคงปลอดภัย ไปจนถึงการลบทำลายข้อมูล เพื่อวัตถุประสงค์ดังนี้

1) เพื่อตรวจสอบผลการปฏิบัติตามกฎหมายให้มีความถูกต้องครบถ้วนอยู่เสมอ

2) เพื่อทบทวนแนวทางการทำงานขององค์กรให้สอดคล้องตามกฎหมายในกรณีที่องค์กรมีกิจกรรมประมวลผลข้อมูลส่วนบุคคลที่เพิ่มขึ้นหรือเปลี่ยนแปลงจากที่มีอยู่เดิม

3) เพื่อเป็นแนวทางป้องกันเหตุอันอาจเกิดได้ในอนาคต

บทที่ 4

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลสำหรับพนักงาน

หลังจากที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการประกาศใช้อย่างเป็นทางการเต็มรูปแบบแล้ว ในวันที่ 1 มิถุนายน พ.ศ. 2565 กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เข้าไปมีบทบาทสำคัญอย่างมากในทุกๆอุตสาหกรรม ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในแง่ของการคุ้มครองแรงงาน มีกิจกรรมต่างๆ และข้อมูลของพนักงานที่กฎหมายดังกล่าวเข้าไปเกี่ยวข้อง โดยไม่จำกัดเพียงแค่ภาครัฐเท่านั้น แต่ยังรวมไปถึงภาคเอกชนที่มีการประมวลผลข้อมูลของพนักงานภายในองค์กรด้วย ในแง่ของการคุ้มครองแรงงาน กฎหมายที่สำคัญที่เข้ามาเกี่ยวข้อง คือ กฎหมายคุ้มครองแรงงาน ไม่ว่าจะเป็นกิจกรรมการคัดเลือกพนักงาน การทำสัญญาจ้างแรงงาน การพัฒนาบุคคลกร การอนุมัติเลื่อนตำแหน่ง หรือแม้แต่การพ้นสภาพการจ้างของพนักงาน กฎหมายดังกล่าวได้เข้าไปมีความเกี่ยวพันทุกกระบวนการ ตัวอย่างเช่น ในกิจกรรมการจัดทำทะเบียนลูกจ้าง ตามพระราชบัญญัติคุ้มครองแรงงาน มาตรา 115 ได้มีการกำหนดระยะเวลาการจัดเก็บข้อมูลของลูกจ้างให้จัดเก็บไว้ไม่เกิน 2 ปี นับแต่วันที่สิ้นสุดการจ้าง จะเห็นได้ชัดว่า การกำหนดระยะเวลาการทำลายข้อมูลดังกล่าวตามกฎหมายคุ้มครองแรงงานได้เข้ามามีบทบาทในการกำหนดรายละเอียดการทำลายข้อมูลส่วนบุคคล ดังนั้น นายจ้างหรือผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ในการดำเนินการลบ หรือทำลาย เมื่อสิ้นระยะเวลาการจัดเก็บดังกล่าว โดยเป็นไปตามหลักการจัดเก็บข้อมูลอย่างจำกัด (storage minimization) หรือ แม้แต่กิจกรรมที่เกี่ยวกับการขอลาของพนักงาน กฎหมายคุ้มครองแรงงาน ได้มีการกำหนดให้นายจ้างสามารถขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่ถ้าเป็นกรณีที่ลาไม่เกิน 3 วันหรือกรณีที่นำไปใช้เพื่อวัตถุประสงค์อื่น นายจ้างมีหน้าที่ต้องขอความยินยอมจากลูกจ้าง เป็นต้น

เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีการประกาศใช้แล้ว จะมีเรื่องการขอใช้สิทธิของลูกจ้างที่เพิ่มมากขึ้น สิทธิของเจ้าของข้อมูลในส่วนของงานฝ่ายทรัพยากรบุคคล หรือ Human Resources (HR) นั้นจะมีอยู่หลายกรณี เช่น สิทธิขอเข้าถึงทะเบียนเอกสาร หรือ การขอสำเนาใบรับรองต่าง ๆ ทั้งใบรับรองเงินเดือน ใบรับรองการทำงานเพื่อนำไปกู้เงิน เป็นต้น เมื่อ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือ PDPA มีผลบังคับใช้แล้ว สิทธิของพนักงานในองค์กรก็จะมีมากขึ้น ดังนั้นบุคลากรในส่วนงาน HR จำเป็นจะต้องเข้าใจสิทธิของพนักงานที่มีเพิ่มขึ้น และเพื่อเป็นการป้องกันเหตุต่าง ๆ ที่อาจจะเกิดขึ้นได้จากการประกาศใช้กฎหมาย บุคลากรในฝ่าย HR ควรเก็บข้อมูลส่วนบุคคลของพนักงานให้อยู่ในประเภทและปริมาณเท่าที่จำเป็นต่อการใช้งานตรงตามวัตถุประสงค์ ซึ่งหมายถึงภาระ/ความรับผิดชอบในการจัดการที่น้อยลงตามไปด้วย

แนวปฏิบัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการคุ้มครองแรงงาน เป็นการแนะนำแนวทางที่ควรปฏิบัติให้กับบริษัท นายจ้าง หรือองค์กร เพื่อดำเนินการให้เป็นไปตามและสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายคุ้มครองแรงงาน โดยกิจกรรมที่เกี่ยวข้องกับการคุ้มครองแรงงานนั้น มีดังนี้

1. กิจกรรมการประกาศรับสมัครและคัดเลือกพนักงาน

การสรรหา และคัดเลือกคนเข้าองค์กร หรือ Recruitment and Selection เป็นขั้นตอนที่มีความสำคัญ เนื่องจากเป็นขั้นตอนแรกที่มีการจัดเก็บข้อมูลส่วนบุคคลของลูกจ้าง ในบางองค์กรโดยเฉพาะองค์กรขนาดใหญ่จะมีแผนกสรรหาบุคลากรที่แยกออกจากแผนกอื่น ๆ โดยเฉพาะ แต่ในบางองค์กรนั้นพนักงานอาจจำเป็นที่จะต้องทำงานในหลายหน้าที่

ในการดำเนินการเกี่ยวกับการสรรหาและคัดเลือกพนักงานสามารถแยกช่องทางการรับสมัครหรือช่องทางการสรรหาพนักงาน ออกได้เป็น 8 ช่องทางดังนี้

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

สิ่งที่นายจ้างควรพิจารณาเพิ่มเติมเกี่ยวกับข้อมูลที่จัดเก็บ ควรมีการเก็บข้อมูลเท่าที่จะเป็น โดยสามารถใช้คำถามดังต่อไปนี้เพื่อสอบถามถึงความจำเป็นในการเก็บข้อมูล ดังนี้

1) ข้อมูลส่วนบุคคลของผู้สมัครอะไรที่บริษัทต้องการ
2) ได้มาจากแหล่งต่างๆ ต้องบริหารจัดการอย่างไร
3) จะเก็บข้อมูลส่วนบุคคลไว้นานเท่าใด
4) เมื่อหมดความจำเป็นจะทำลายอย่างไร

[หน้าที่นายจ้างในการแจ้งต่อผู้สมัคร] เมื่อผู้สมัครได้รับการตอบรับการสมัครงาน จะมีการจัดเก็บข้อมูลส่วนบุคคลของผู้สมัครงาน รวมถึงข้อมูลละเอียดอ่อนที่อาจเข้ามาเกี่ยวข้องเช่น การเก็บข้อมูลสุขภาพ การเก็บข้อมูลศาสนา นอกจากบริษัทมีหน้าที่ในการต้องแจ้งประกาศความเป็นส่วนตัวในขั้นตอนการประกาศโฆษณาและในขั้นตอนการกรอกใบสมัครเมื่อผ่านการคัดเลือกนั้น ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งประกาศความเป็นส่วนตัวให้ผู้สมัครงานทราบอีกครั้ง แต่จะมีความแตกต่างในเรื่องของข้อมูลที่มีการจัดเก็บ และวัตถุประสงค์ในกรจัดเก็บ รวมถึงรายละเอียดในการแจ้งที่แตกต่างออกไปจาก ขั้นตอนที่มีการส่งตอนที่มีการโฆษณารับสมัครงาน สิทธิในการได้รับแจ้ง เจ้าของข้อมูลส่วนบุคคลต้องได้รับการแจ้งให้ทราบก่อนหรือขณะเก็บข้อมูล ตามมาตรา 23 ดังนี้

1) วัตถุประสงค์ในการเก็บและฐานทางกฎหมาย
2) กรณีต้องใช้ข้อมูลส่วนบุคคล เพื่อปฏิบัติตามกฎหมายหรือตามสัญญา
3) การเก็บขอมูลนั้นเป็นการเก็บอะไร เก็บนานเท่าไหร่
4) จะมีการเปิดเผยข้อมูลให้หน่วยงานหรือบุคคลใดบ้าง
5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล สถานที่ติดต่อ วิธีการติดต่อ รวมถึงรายละเอียดของผู้เป็น DPO (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)
6) สิทธิของเจ้าของข้อมูลส่วนบุคคล

2. กิจกรรมการทำสัญญา หรือ Employee Contract

หลังจากที่ได้รับการคัดเลือกเป็นพนักงานแล้วก็จะเข้าสู่ขั้นตอนการทำสัญญาจ้างงานและสัญญาที่เกี่ยวข้องกับการจ้างแรงงานที่มีหลากหลายรูปแบบ ไม่ใช่เพียงแค่สัญญาจ้างแรงงานเพียงเท่านั้นแต่ยังมีสัญญาการจ้างอื่น ๆ ซึ่งแตกต่างจากสัญญาจ้างแรงงานทั่วไป ตัวอย่างสัญญาจ้างมีดังต่อไปนี้

1. สัญญาจ้างงาน เป็นสัญญาที่ทำขึ้นระหว่างฝ่ายนายจ้าง และฝ่ายพนักงาน โดยเป็นสัญญาต่างตอบแทนในหน้าที่ และค่าจ้าง โดยมีข้อกำหนดในเรื่องค่าตอบแทน สวัสดิการ และสิทธิประโยชน์ต่างๆ ตามที่กฎหมายกำหนดไว้

2. สัญญารับจ้างทำของ ในสัญญาการจ้างทำของนั้นมักเกิดขึ้นในการทำงานในรูปแบบของการจ้างผู้มีอาชีพอิสระให้ทำงานให้ หรือที่เรียกว่า “freelance” โดยในส่วนนี้อาจจะไม่ได้มาจากขั้นตอนว่าจ้างหรือการสรรหา แต่อาจจะเป็นการตกลงกัน มีการประมูลมีการว่าจ้างกันเป็นรายกรณี ในสัญญารับจ้างทำของ จะไม่คำนึงถึงในเรื่องระยะเวลาการทำงานแต่จะเน้นที่ผลลัพธ์ของผลงานที่ผู้ว่าจ้างต้องการ แต่ในสัญญาจะมีการแจ้งวัตถุประสงค์ในการทำกิจกรรมเพื่อให้ได้ผลงานออกมาตามที่ผู้ว่าจ้างต้องการ เช่น แผนกขนส่งมีออเดอร์เยอะเกินไป แต่ระบบการขนส่งของบริษัทมีไม่เพียงพอ จึงดำเนินการจ้าง Outsource เข้ามาดำเนินงาน และทำให้งานคล่องตัว และได้ความสำเร็จตามที่บริษัทต้องการ เป็นต้น

3. สัญญาค้ำประกัน ในความหมายตามบริบทนี้ การทำสัญญาค้ำประกัน มี 2 รูปแบบ คือ ค้ำประกันการทำงาน หรือ ค้ำประกันค่าความเสียหายจากการทำงาน ซึ่งหากเป็นสัญญาค้ำประกันตามกฎหมายแรงงาน กฎหมายมิได้หมายความว่าการค้ำประกันจะสามารถทำได้ทุกตำแหน่ง การค้ำประกันจะทำได้เฉพาะในตำแหน่งที่มีหน้าที่รับผิดชอบทางการเงินโดยตรงหรือผู้ดูแลทรัพย์สินเท่านั้น

4. สัญญาระหว่างบริษัท กับ บริษัทจัดหาแรงงาน ในบางบริษัทจะมีการใช้การจ้างงานแบบชั่วคราว (Outsource) เป็นสัญญาการบริการระหว่างผู้ค้ากับหน่วยธุรกิจ หรือ Business to Business (B2B) และใช้กันอย่างแพร่หลายโดยเฉพาะธุรกิจอุตสาหกรรมขนาดใหญ่ เช่น อุตสาหกรรมการก่อสร้าง หรือโรงงานอุตสาหกรรม และแม้กระทั่งแรงงานในสำนักงาน เป็นต้น

สัญญาในรูปแบบนี้ควรมีการตั้งประเด็นคำถามเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ดังต่อไปนี้

- การทำสัญญาระหว่างผู้ให้บริการ และบริษัทผู้ว่าจ้าง มีกิจกรรมใดที่เกี่ยวข้องกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่
- บริษัทผู้ว่าจ้างที่ใช้แรงงานที่ส่งมาจากบริษัทผู้รับเหมา มีการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ ผู้ว่าจ้างต้องตรวจสอบว่าบริษัทที่ส่งผู้ใช้แรงงาน หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น แล้วผู้ใดเป็นคนเก็บ มีมาตรการเช่นใด

5. สัญญาส่งไปฝึกงานหรือทำงานต่างประเทศ บริษัทที่มีสำนักงานเครือข่ายหรือมีสาขาอยู่ในหลาย ๆ ประเทศ หรือ บริษัทที่จะต้องส่งพนักงานไปเรียนรู้กระบวนการทำงานและเทคนิคต่าง ๆ ของบริษัทแม่ หรือ บริษัทในเครือนั้น สามารถทำเป็นสัญญาฝึกงานหรือสัญญาส่งตัวไปทำงาน/ฝึกงานต่างประเทศได้ แต่มีข้อควรระวังใน 2 มาตรา คือ มาตรา 28 และมาตรา 29 โดยหลักการคือ การส่งข้อมูลส่วนบุคคลไปยังต่างประเทศหรือนอกราชอาณาจักรนั้น ประเทศปลายทางนั้นๆต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ที่เพียงพอ ไม่ต่ำกว่าของประเทศไทย หรือมีความใกล้เคียงกับของประเทศไทย

6. สัญญาจ้างนักเรียน นักศึกษาในการทำงานแบบชั่วคราว (Part time) ในสัญญาการจ้างนักเรียน หรือ นักศึกษามาทำงาน Part time นั้น เป็นการทำงานหลังเลิกเรียน และไม่ได้เป็นลูกจ้างทำงานประจำในเวลางาน

การทำงาน Part time หมายถึง การทำงานนอกเวลาเรียน ซึ่งรวมถึงการทำงานในวันเสาร์ – อาทิตย์หรือบางครั้งในวันหยุดด้วย จึงจะต้องมีระเบียบข้อบังคับ หรือข้อกำหนดที่เข้มงวดว่านักเรียนหรือนักศึกษาที่จะทำงานให้บริษัทนั้นทั้งนอกเวลาและในวันหยุด สามารถทำงานได้ไม่เกินวันละกี่ชั่วโมง หรือ เมื่อทำงานในวันธรรมดาของช่วงปิดเทอมจะสามารถทำได้ไม่เกินกี่ชั่วโมง โดยข้อควรระวังนั้นผู้ว่าจ้างควรตรวจสอบอายุของนักเรียนนักศึกษาเพื่อไม่ให้เกิดความผิดพลาดทางข้อกฎหมายหากผู้ถูกว่าจ้างเป็นผู้เยาว์

ข้อตกลงการรับนักศึกษาเข้าฝึกงาน (MOU ระหว่างบริษัท กับสถาบันการศึกษา) ปัจจุบันสถาบันการศึกษาต่าง ๆ มีการทำสัญญา MOU กับบริษัทหรือหน่วยงานเพื่อส่งตัวนักเรียนนักศึกษามาฝึกงาน โดยระบุให้มีการเซ็นสัญญาช่วงที่ต้องการฝึกงานตามหลักสูตรของรายวิชานั้น ๆ

ในกรณีนี้ทางสถาบันการศึกษาจะเป็นผู้เซ็นสัญญาร่วมกับบริษัท แต่ตัวผู้ฝึกงานซึ่งเป็นนักเรียน นักศึกษา นั้นจะไม่ได้อยู่ในสถานะลูกจ้าง อย่างไรก็ตาม ทางบริษัทหรือฝ่ายทรัพยากรบุคคล จะต้องมีการเก็บข้อมูลส่วนบุคคล ประวัตินักเรียนนักศึกษา เช่น ข้อมูลสถาบัน ปีที่เข้าร่วมงาน แผนกที่ทำงาน ช่วงเวลาในการทำงาน ซึ่งการเก็บข้อมูลนักเรียนนักศึกษาถือเป็นขั้นตอนที่ควรต้องระมัดระวัง และมีความสำคัญเทียบเท่ากับการเก็บรวบรวมประวัติของพนักงาน โดยเฉพาะข้อมูลส่วนบุคคลประเภทละเอียดอ่อนนั้นควรเก็บเท่าที่จำเป็น และหากบริษัทจะต้องเก็บไฟล์สแกนลายนิ้วมือ กลุ่มเลือด หรือการสแกนใบหน้า ของนักเรียนนักศึกษา ทางฝ่ายทรัพยากรบุคคลต้องมีมาตรการและขั้นตอนเหมือนพนักงาน และนอกเหนือจากนั้นเนื่องจากผู้เยาว์จะต้องให้ความยินยอมและความสมัครใจด้วยตนเอง เพิ่มเติมการให้ความยินยอมเป็นการเฉพาะสำหรับผู้เยาว์

7. สัญญาจ้างงานผู้พิการ ในกรณีที่ทางบริษัทจ้างงานผู้พิการ ซึ่งเป็นการจ้างงานบุคคลผู้พิการตาม พระราชบัญญัติส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ พ.ศ.2550 (พนักงานผู้พิการ 1 คน ต่อพนักงาน 100 คน) ปัจจุบันการทำสัญญาการจ้างงานสามารถทำได้เพราะเป็นฐานของกฎหมาย หากในการเก็บรวบรวม ใช้ หรือเปิดเผย จัดเก็บ การลบและการทำลายข้อมูลส่วนบุคคล จะเป็นไปในขั้นตอนเทียบเท่าการจ้างพนักงาน หากแต่เพิ่มการให้คำยินยอมสำหรับผู้พิการโดยเฉพาะ

เอกสารที่ใช้ประกอบในขั้นตอนการทำสัญญาจ้างแรงงาน

เอกสารที่ในการประกอบการทำสัญญานั้น ประกอบไปด้วยข้อมูลส่วนบุคคล ซึ่งมีทั้งข้อมูลส่วนบุคคลละเอียดอ่อน และข้อมูลส่วนบุคคลทั่วไป โดยทั่วไปแล้วในกิจกรรมการทำสัญญาการจ้างงานประกอบไปด้วยเอกสารดังต่อไปนี้

1) หน้าสมุดบัญชีธนาคาร จากขั้นตอนการคัดเลือกและสรรหาที่ผ่านมาแล้วนั้น บริษัทควรพิจารณาว่าเอกสารใดจำเป็นที่ต้องใช้แนบสำหรับสัญญาจ้างงาน หรือเอกสารใดที่ไม่จำเป็น เช่น จำเป็นหรือไม่ที่ต้องขอเอกสารหน้าบัญชีธนาคารตั้งแต่วันแรกที่พนักงานเข้ามาสมัครงานแต่จะเป็นสำหรับผู้ที่ผ่านการสัมภาษณ์งานและเซ็นสัญญาแล้วเท่านั้น

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

3) การตรวจสุขภาพ การตรวจสอบประวัติอาชญากรรม หากบริษัทต้องการเก็บข้อมูลส่วนบุคคลละเอียดอ่อนบางรายการ จะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่น การขอตรวจสุขภาพ การขอตรวจประวัติอาชญากรรม การเก็บลายนิ้วมือจากการสแกน ซึ่งกระบวนการเหล่านี้จะต้องดำเนินการอย่างเป็นขั้นตอนและแจ้งวัตถุประสงค์ต่อเจ้าของข้อมูลให้ชัดเจน หรืออาจต้องมีการขอความยินยอมอื่น ๆ ในบางกรณี เช่น การใช้จีพีเอสติดตามตัวก็ถือว่าเป็นอีกหนึ่งรายการซึ่งไม่ใช่ข้อมูลส่วนบุคคลละเอียดอ่อน แต่การใช้จีพีเอสติดตามอาจจะเป็นละเมิดข้อมูลส่วนบุคคลได้ แต่หากจีพีเอสนั้นนำใช้งานกับเครื่องมือหรืออุปกรณ์อื่นๆ เช่น รถของบริษัท หรือรถของส่วนกลางที่ขับขี่ออกไป ในกรณีนี้ถือว่า เป็นมาตรการของบริษัทสำหรับพนักงานผู้ทำหน้าที่ แต่หากรถติดจีพีเอสแล้วให้นำไปใช้งานวันหยุดเสาร์-อาทิตย์ก็จะสามารถตรวจสอบที่อยู่ได้ แบบนี้จะเป็นการเข้าไปละเมิดสิทธิส่วนบุคคลมากเกินไป

เอกสารที่บริษัทต้องจัดทำเมื่อมีการทำสัญญาจ้างกับพนักงาน ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้แก่

1. ประกาศความเป็นส่วนตัวสำหรับพนักงาน
2. หนังสือขอความยินยอม
3. บันทึกรายการประมวลผลข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

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

1) วัตถุประสงค์

2) ความจำเป็นต้องให้ข้อมูล

3) ข้อมูลที่จัดเก็บระยะเวลาการจัดเก็บ

4) ประเภทของบุคคลหรือนิติบุคคลที่ข้อมูลอาจจะต้องมีการเปิดเผย

5) ข้อมูลตัวแทนของผู้ควบคุมข้อมูล

6) สิทธิตามกฎหมาย

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

1.2 กรณีการเก็บข้อมูลพนักงาน โดยเมื่อพนักงาน ผ่านการสัมภาษณ์แล้ว บริษัทจะมีการเก็บข้อมูลพนักงานเพิ่มเติม โดยอาจแจ้งแนบไปกับสัญญาจ้างงาน หรืออาจใช้รูปแบบ QR Code เพื่อให้การเข้าถึงเอกสารนั้นง่ายขึ้น

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 หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

การขอความยินยอม ต้องระบุวัตถุประสงค์ให้ชัดเจน เข้าใจง่าย ไม่คลุมเครือ และทำให้ผู้ให้ความยินยอมให้ความยินยอมโดยสมัครใจ 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, RoPA) ตามมาตรา 39

การทำบันทึกรายการกิจกรรมนี้เป็นไปตามข้อกำหนดใน พรบ. และเป็นหน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล โดยต้องมีการบันทึกในรายละเอียด เพื่อเป็นหลักฐานและในกรณีต้องมีการตรวจสอบบันทึกการประมวลผลข้อมูลส่วนบุคคล ได้แก่ ข้อมูลที่มีการเก็บรวบรวม, วัตถุประสงค์ในการเก็บ, ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล, ระยะเวลาในการเก็บรักษา, สิทธิเจ้าของข้อมูล, การปฏิเสธการใช้สิทธิ, คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และเพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตรวจสอบได้

หน้าที่ในการจัดทำทะเบียนลูกจ้าง 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

3. กิจกรรมการใช้ข้อมูลของพนักงานร่วมกันในหลายบริษัท

1. ใช้ข้อมูลพนักงานร่วมกันในเครือบริษัทที่อยู่ในประเทศไทย

บริษัทในเครือเดียวกันหากอยู่ในประเทศไทยทั้งหมด ก็จะอยู่ภายใต้กฎหมาย PDPA เดียวกันในกรณีที่บริษัทั้งหมดในเครืออยู่ในประเทศไทย การแบ่งหรือใช้ข้อมูลร่วมกัน (Sharing) สามารถใช้ฐานเดียวกันได้ คือฐานสัญญา

การเปิดเผยข้อมูลออกไปยังบริษัทในเครือได้ จะต้องแจ้งกับพนักงานว่า อาจจะต้องมีการส่งข้อมูลออกไปให้กับบริษัทในเครือ หากบริษัทในเครือใช้นโยบายเรื่องการคุ้มครองข้อมูลส่วนบุคคล และนโยบายความเป็นส่วนตัวที่เป็นฉบับเดียวกันทั้งหมดก็ สามารถดำเนินการได้ แต่หากบริษัทในเครือมีนโยบายของตนเอง การแชร์ข้อมูลของพนักงาน จะต้องมีการตรวจสอบมาตรการ และขั้นตอน รวมทั้งมาตรฐานทางระบบก่อน

การแจ้ง Privacy Notice หรือ การแจ้งตามมาตรา 23 ฐานทางกฎหมายที่ใช้ (Lawful Basis) **เป็นฐานสัญญา** ระบุให้ชัดเจนว่าจะเปิดเผยข้อมูลส่วนบุคคลอะไรบ้าง ไปยังบริษัทที่อยู่ในเครือบริษัทใด กรณีบริษัทในเครือแยกนโยบายคุ้มครองข้อมูลส่วนบุคคลกันคนละฉบับ ต้องแจ้งนโยบายของบริษัทในเครือให้พนักงานบริษัททราบด้วย

ความรับผิดชอบในฐานะ **“ผู้ควบคุมข้อมูลส่วนบุคคล”** เป็นของบริษัทต้นสังกัดที่พนักงานอยู่ในสังกัด ในประเทศไทยจึงอยู่ในข้อบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่นกัน

2. การใช้ข้อมูลพนักงานร่วมกันในเครือบริษัทที่อยู่ในต่างประเทศ

ในกรณีที่บริษัทในเครืออยู่ต่างประเทศ จะเข้ากับข้อกฎหมายตามมาตรา 28 และ มาตรา 29 เพราะเมื่อส่งข้อมูลออกไปยังต่างประเทศ จำเป็นต้องมีการตรวจสอบประเทศปลายทางในส่วนของหลักการทางกฎหมาย โดยประเทศปลายทางจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกับประเทศไทย หรือไม่ด้อยไปกว่าของไทย ตัวอย่างเช่น การส่งข้อมูลจากประเทศในกลุ่ม Europe กลุ่ม EU ไปยังประเทศ Singapore หรือจาก America ไป England และ Australia กลุ่มประเทศเหล่านี้จะมี Data Protection คล้ายกับประเทศไทย แต่หากส่งออกข้อมูลไปในประเทศที่ไม่มั่นใจในเรื่องของการคุ้มครองข้อมูล (Data Protection) จำเป็นต้องมีการตรวจสอบรายละเอียดก่อนทำการส่งข้อมูล

หากเป็นบริษัทในเครือของบริษัทสำนักงานใหญ่ โดยปกติจะมีเอกสารที่เรียกว่า Binding Corporate Rules ซึ่งเป็นเสมือนกับเป็นบัญญัติที่ใช้กับทุกๆบริษัทในเครือ เช่น บริษัทของญี่ปุ่น บริษัทแม่อยู่ญี่ปุ่นแต่มีสาขาย่อยทั่วโลก บริษัทลูกจะเปิดใช้บัญญัติฉบับเดียวกันและมีมาตรฐานก็จะเป็นในแนวทางก็สามารถดำเนินการได้ แต่หากมีเหตุต้องส่งข้อมูลส่วนบุคคลออกไปในบริษัทที่อยู่ในประเทศที่มีมาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอหรือยังไม่มี จำเป็นต้องแจ้งให้พนักงานทราบว่าประเทศนี้ยังไม่มีมาตรฐานหรือยังไม่เปิดใช้งาน Data Protection เพื่อให้พนักงานได้ตัดสินใจก่อนจะเซ็นยินยอม

การแจ้ง Privacy Notice หรือการแจ้งตามมาตรา 23 โดยฐานทางกฎหมายที่ใช้ (Lawful Basis) เป็นฐานสัญญา ต้องระบุให้ชัดเจนว่าจะเปิดเผยข้อมูลส่วนบุคคลอะไรบ้าง บริษัทผู้ส่งข้อมูลส่วนบุคคลออกไปยังต่างประเทศต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ดีเพียงพอหรือมีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและอนุมัติจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว (มาตรา 28, 29) บริษัทผู้ส่งข้อมูลส่วนบุคคลออกไปยังต่างประเทศต้องตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทาง (มาตรา 28) ถ้ายังไม่ดีเพียงพอต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเพื่อขอความยินยอมก่อน ความรับผิดชอบในฐานะ “ผู้ควบคุมข้อมูลส่วนบุคคล” เป็นของบริษัทที่พนักงานสังกัดควรจัดทำเอกสาร Binding corporate rules (BCR)

3. การใช้ข้อมูลพนักงานร่วมกันระหว่างบริษัท กับ บริษัทจัดหาแรงงาน

ในบางกรณีการใช้ลูกจ้างเหมาค่าแรงแบบ Outsource อาจจะต้องใช้ข้อมูลจากทั้งสองฝ่าย ทั้งในส่วนของบริษัท Outsource และพนักงานเองซึ่งหากมีขั้นตอนการทำงานแบบนี้ทางบริษัทต้องมีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่คุ้มครองไปยังลูกจ้าง outsource ด้วย

1) มีกิจกรรมที่เกี่ยวข้องกับการ เก็บรวบรวม ใช้ เปิดเผย และ ต่างฝ่ายต่างเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” Data Controller (DC)

2) ต่างฝ่ายต้องแจ้ง Privacy Notice หรือ การแจ้งตามมาตรา 23 ให้พนักงานรับเหมาค่าแรงทราบ

3) ระหว่าง บริษัท กับ บริษัทจัดหาแรงงาน ควรจัดทำ “สัญญาแบ่งปันข้อมูล” Personal Data Sharing Agreement

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

4. การใช้ข้อมูลพนักงานร่วมกันระหว่าง “ผู้ควบคุมข้อมูล” กับ “ผู้ประมวลผลข้อมูล”

การแบ่งปันข้อมูลระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลนั้นอยู่ในส่วนของมาตราต่าง ๆ เช่น การตรวจสุขภาพให้พนักงาน การส่งข้อมูลให้สถานพยาบาลที่รับตรวจ โดยการส่งต้องเป็นข้อมูลทั่วไป ไม่ใช่ข้อมูลที่ละเอียดอ่อน เมื่อตรวจสุขภาพ บริษัทควรให้พนักงานใช้แค่ 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

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

4. การประเมินผลงานของพนักงาน

การประเมินผลพนักงานโดยหลักที่เราพบเป็นประจำและใช้งานกันมีอยู่ 5 รายการ ดังนี้

1. การประเมินสัมภาษณ์งาน

เป็นการประเมินคุณสมบัติและคุณลักษณะเบื้องต้นสำหรับตำแหน่งงาน

2. การประเมินผลระยะทดลองงาน

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

3. การประเมินผลงานประจำปี

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

4. การประเมินเพื่อปรับเลื่อนตำแหน่ง การประเมินผลในรูปแบบนี้อาจจะต้องมีการนำผลการประเมินผลงานหลายปีย้อนหลัง เช่น 2-3 ปีหลังมาพิจารณาด้วย ว่าได้มีผลการประเมินดีมาตลอดจึงควรได้รับการเลื่อนตำแหน่ง หรือเมื่อเลื่อนตำแหน่งไปแล้วพนักงานสามารถทำได้ตามตำแหน่งหรือไม่ และทำได้ตามความสามารถที่คาดหวังไว้หรือไม่

5. การประเมินเมื่อมีการเปลี่ยนงาน เช่น พนักงานย้ายจากแผนกหนึ่งมาอีกแผนกหนึ่ง หรือ อาจจะย้ายการทำงานที่มีลักษณะใกล้เคียงกัน แต่อาจจะต้องมีการประเมินใหม่อีกครั้งว่าพนักงานยังมีศักยภาพในการทำงานเหมือนเดิมหรือไม่

หลักการโดยทั่วไปของการประเมินผลพนักงานมี ประมาณ 5 เรื่อง ดังนี้

1) หัวข้อในการประเมินต้องเกี่ยวข้องกับการคัดเลือกคน

2) การให้ความคิดเห็นของกรรมการสัมภาษณ์ต้องระมัดระวัง

3) ไม่เปิดเผยให้ผู้ที่ไม่เกี่ยวข้องทราบถึงข้อมูล

4) เจ้าของข้อมูลส่วนบุคคลมีสิทธิตาม PDPA ในข้อมูลส่วนบุคคล

5) การทำลายเมื่อหมดความจำเป็น

กรณีตัวอย่างการประเมินพนักงาน

1. ตัวอย่างการประเมินหัวข้อเรื่องของการคัดเลือกพนักงาน

การคัดเลือกพนักงานจะมีการกำหนดคุณสมบัติที่บริษัทต้องการ และมีพื้นที่ให้แสดงความคิดเห็นสำหรับผู้สัมภาษณ์ โดยปกตินั้นผู้สัมภาษณ์ก็ไม่ใช่แค่ HR ฝ่ายเดียว แต่ก็จะมีผู้จัดการฝ่าย หรือหัวหน้าฝ่ายนั้น ๆ เข้าร่วมในการสัมภาษณ์ด้วย เพราะฉะนั้นจุดที่สำคัญคือเมื่อเราต้องการคัดเลือกคนเข้าทำงาน ประเด็นคำถามควรเป็นหัวข้อที่สัมพันธ์กับการทำงานและการเขียนความคิดเห็นที่หัวหน้าเขียนก็จะต้องสัมพันธ์กับตำแหน่งการทำงานเช่นกัน ซึ่งผู้สมัครที่เข้ารับการสัมภาษณ์มีสิทธิในการขอดูใบประเมินได้ว่าเหตุใดจึงไม่ผ่านการสัมภาษณ์งาน

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

ในเรื่องของการประเมินผลงานประจำปีก็จะมีเนื้อหาที่ใกล้เคียงกัน แบบฟอร์มควรมีการระบุเป็นหัวข้อและในช่องที่เป็นตัวเลขให้ใช้คำ ว่า “พอใช้”“ดี” “ดีมาก” และไม่ควรใช้ว่า “ดีมากกว่า” “ดีมาก” “ดีพอใช้” “ควรปรับปรุง” ซึ่งรูปแบบนี้เราก็ต้องมีหลักฐานและมีการแสดงความคิดเห็นที่ถูกต้องตามเรื่องของการทำงาน โดยส่วนมากการประเมินเราจะต้องให้ feedback กับพนักงานว่าต้องพัฒนาอะไร และเมื่อมีการให้ Feedback ขั้นตอนต่อไปคือการให้ความรู้ความเข้าใจกับทางหัวหน้างานว่าพนักงานนั้นมีสิทธิในการที่จะขอดูผลการประเมิน เพราะฉะนั้นเวลาดำเนินการจะต้องโปร่งใสและเป็นธรรม โดยผลการประเมินต่าง ๆ ควรมีการเก็บประมาณ 2-3 ปี

5. การบันทึกเวลาของพนักงานในรูปแบบต่างๆ

ในสมัยก่อนนั้นการบันทึกเวลาจะเป็นในรูปแบบของบัตรตอก การรูดบัตร และการใส่รหัส ซึ่งปัจจุบันมีเทคโนโลยีใหม่ ๆ เกิดขึ้นตลอดเวลา เช่น

1) Finger Scan (การสแกนลายนิ้วมือ)

2) Face Recognition (การจดจำใบหน้า)

3) Iris Recognintion (การจดจำรูม่านตา)

4) Voice Recognition (การจดจำเสียง)

5) การสแกนเส้นเลือดดำบนฝ่ามือ

ข้อมูลทั้งหมดนี้ถือเป็นข้อมูลทางชีวภาพ หรือ Biometric ซึ่งเป็นข้อมูลละเอียดอ่อนที่จำเป็นต้องปกป้องสูงกว่าข้อมูลทั่วไป เนื่องจากใช้ในการปลอมแปลงตัวตนได้ การเก็บข้อมูลเหล่านี้ จัดอยู่ในกลุ่มมาตรา 26 ห้ามมิให้เก็บข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

การสแกนลายนิ้วมือ Finger Scan เสถียรภาพไม่ค่อยดี สามารถปลอมแปลงได้ง่ายกว่า การจดจำใบหน้า Face Recognition ในขณะที่การสแกนรูม่านตา ก็พัฒนาขึ้น สามารถแบ่งแยกฝาแฝดได้ เนื่องจากโครโมโซมไม่เหมือนกัน แต่การสแกนรูม่านตาบ่อย ๆ อาจส่งผลต่อม่านตาได้ จึงไม่ค่อยใช้ในอุตสาหกรรมหรือบริษัททั่วไป 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 เว้นแต่เข้าข้อยกเว้นตามบัญญัติของพ.ร.บ.ฉบับนี้

6. การเก็บข้อมูลเพื่อบันทึกเวลาการเข้างาน

กรณี “ไม่ต้องขอความยินยอม” : บัตรตอก บัตรรูด ใส่รหัส ลงสมุดเข้างาน

กรณี “ต้องขอความยินยอม” : Biometric สแกนนิ้วมือ สแกนใบหน้า สแกนม่านตา

กรณีศึกษาฐานทางกฎหมายที่ใช้ในการบันทึกเวลาทำงานของพนักงาน

บริษัทแห่งหนึ่ง มีโรงงานหลายแห่ง และมีวิศวกรโยธาหลายคน ซึ่งทำงานไม่พร้อมกัน และทำให้ต้องมีรถประจำตำแหน่งเพื่อสะดวกในการเดินทาง บริษัทจึงมีการติด GPS ในรถ เพื่อดูรายงานการเข้าออกงาน ในกรณีดังกล่าว สามารถดำเนินการโดยใช้ ฐาน Legitimate Interest เนื่องจากมีเหตุผลที่เพียงพอและพอรับได้ว่าเพื่อใช้ในการคิดค่าทำงานล่วงเวลา แต่ในกรณีนี้ข้อควรระวัง คือ จะทำอย่างไรเพื่อไม่ให้เป็นการละเมิดความเป็นส่วนตัวหลังเลิกงาน วิธีที่ดีที่สุด คือ ปิดการติดตาม GPS ตอนเลิกงาน แต่อาจเป็นเรื่องยุ่งยากพอสมควร ดังนั้นการขอความยินยอม จึงเป็นอีกแนวทางหนึ่งในการดำเนินการในกรณีดังกล่าว โดยจะต้องออกแบบขั้นตอนในการเก็บข้อมูลให้ดี เพื่อให้พนักงานมั่นใจว่าจะไม่เกิดการละเมิดสิทธิ์ส่วนบุคคล

ในการขอความยินยอมนั้น สามารถขอความยินยอมในวันทำสัญญาเข้าทำงาน โดยความยินยอมจะต้องไม่เป็นส่วนใดส่วนหนึ่งของสัญญา เช่น การแยกเอกสารขอความยินยอมโดยเฉพาะ เพื่อให้มั่นใจว่าความยินยอมนั้นไม่ใช่ส่วนหนึ่งของสัญญาและในการขอความยินยอมสามารถอธิบายถึงความจำเป็นต้องเก็บ โดยแต่ละบริษัทอาจมีเอกสารขอความยินยอมที่แตกต่างกัน ทั้งนี้ในการขอความยินยอมสามารถแบ่งออกเป็นเรื่อง ๆ เช่น การเก็บข้อมูลด้านสุขภาพ ขอความยินยอมการตรวจข้อมูลประวัติอาชญากรรม ขอความยินยอมในการสแกนใบหน้าเพื่อรายงานการเข้าออกบริษัทและนอกจากหนังสือขอความยินยอมเมื่อเข้าทำงานแล้ว ในกรณีที่พนักงานลาออกควรลบทำลายข้อมูลทันทีเมื่อหมดความจำเป็น บริษัทอาจจะต้องเตรียมแบบฟอร์มและขั้นตอนการขอถอนความยินยอมในกรณีที่พนักงานต้องการ โดยจะต้องออกแบบให้สามารถถอนความยินยอมได้ง่ายเหมือนกับการขอความยินยอมตอนเข้าทำงานเช่นกัน

7. การตรวจสุขภาพของพนักงานและใบรับรองแพทย์

การตรวจสุขภาพของพนักงานถือเป็นสิ่งที่สำคัญเพราะนอกจากจะเป็นหน้าที่หลักของงาน HR แล้ว การตรวจสุขภาพยังมีความเกี่ยวข้องกับข้อมูลละเอียดอ่อน ซึ่งมีด้วยกันหลายประเภท 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 นายจ้างอาจขอใบรับรองแพทย์จากลูกจ้างที่ลาป่วยตั้งแต่ 3 วันขึ้นไป แต่หาก กรณีลาป่วยไม่เกิน 3 วัน และนายจ้างขอใบรับรองแพทย์จากลูกจ้างหรือ กรณีนายจ้างขอใบรับรองแพทย์เพื่อนำไปใช้วัตถุประสงค์อย่างอื่น จำเป็นจะต้องจัดทำหนังสือขอความยินยอม

8. การให้สวัสดิการกับการเก็บข้อมูลส่วนบุคคล

สวัสดิการนั้นเป็นส่วนหนึ่งในการจูงใจให้พนักงานทำงานกับบริษัทและยังช่วยให้รับพนักงานใหม่ได้ง่ายขึ้น สวัสดิการนั้นอยู่นอกเหนือกฎหมาย ขึ้นอยู่กับแต่ละบริษัท ซึ่งในปัจจุบันแต่ละบริษัทมีสวัสดิการมากมาย ซึ่งมีส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. สวัสดิการแต่งงาน คลอดบุตร งานศพ

ในส่วนนี้ต้องดูว่าบริษัทมีขั้นตอนในการดำเนินงานการเบิกจ่ายสวัสดิการอย่างไร ถ้าให้เบิกได้เลยโดยไม่ต้องใช้เอกสารใด ๆ จะไม่มีส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่ถ้าต้องมีเอกสารแนบ เช่น สูติบัตร ถือเป็นการเก็บข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์ จึงจำเป็นต้องมีการขอความยินยอม ซึ่งผู้ปกครองส่วนใหญ่ย่อมอยากจะได้สวัสดิการและยินดีในการให้ความยินยอม หรือในกรณีพนักงานแต่งงาน หากทางบริษัทต้องใช้ทะเบียนสมรสเป็นหลักฐาน ถือเป็นการเก็บข้อมูลส่วนบุคคลของบุคคลที่สาม ซึ่งต้องใช้การขอความยินยอมเช่นกัน

2. การท่องเที่ยวประจำปี การแข่งกีฬา งานเลี้ยงปีใหม่ งานเลี้ยงเกษียณ

ส่วนที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ การถ่ายรูป ทั้งนี้คนไทยส่วนใหญ่จะชอบการถ่ายรูป แต่อาจจะมีบางคนที่ไม่ชอบให้มีการเผยแพร่ในสื่อต่าง ๆ ดังนั้นจึงจะต้องเคารพสิทธิของคนกลุ่มดังกล่าว จึงควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคล ไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆ เช่น การขอลบ เป็นต้น

3. งานเลี้ยงวันเกิดแจกของ

ในแต่ละเดือน บางบริษัทจะมีการเปิดเผยชื่อพนักงานที่เกิดในเดือนนั้น ๆ และการจัดกิจกรรมวันเกิด ซึ่งอาจจะมีบางคนที่ไม่ต้องการให้มีการเปิดเผยเช่นกัน ดังนั้นจึงควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคล ไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆค่อยมีประเด็นเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล

4. กองทุนสำรองเลี้ยงชีพ

ในส่วนของกองทุนสำรองเลี้ยงชีพนั้น ส่วนใหญ่จะแค่เปิดเผยข้อมูลไปยังผู้จัดการกองทุนเท่านั้น ซึ่งเป็นข้อมูลทั่วไป จึงไม่ค่อยมีประเด็นเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล

5. การลาพิเศษในวันสำคัญทางศาสนา

ในการเก็บข้อมูลทางศาสนากรณีที่มีความจำเป็น เช่น เพื่อให้วันหยุดเพิ่มตามศาสนา ทั้งนี้บริษัทสามารถขอความยินยอมให้พนักงานให้ข้อมูลหลังจากได้รับการคัดเลือกเป็นพนักงาน เพื่อเป็นสิทธิประโยชน์ในการลาของพนักงาน แต่อย่างไรก็ตามพนักงานมีสิทธิ์ที่จะให้หรือไม่ให้ก็ได้ แต่ไม่จำเป็นต้องขอความยินยอมตั้งแต่ตอนสมัคร เพราะจะส่งผลต่อการจัดการในกรณีที่ผู้สมัครงานไม่ได้รับการคัดเลือก

ทั้งนี้หากเป็นกรณีมีการจัดกิจกรรมที่ต้องจัดเตรียมอาหาร จัดห้องพิเศษ เช่น เพื่อการละมาด บริษัทไม่จำเป็นต้องขอข้อมูลทางศาสนา แต่สามารถถามความต้องการในเรื่องของ Facility เพิ่มเติม ให้พนักงานแจ้งเอง โดยเลี่ยงการขอข้อมูลทางศาสนา

6. ค่าเดินทางหรือจัดรถรับส่ง

การให้ค่าเดินทาง หรือการจัดรถรับส่งพนักงาน บริษัทควรมีการแจ้งการคุ้มครองข้อมูลส่วนบุคคล ไว้ก่อนการเก็บรวบรวม ใช้ หรือมีการเปิดให้ใช้สิทธิต่าง ๆ เช่นขอเก็บข้อมูล ที่อยู่บ้าน หรือตำแหน่งบ้าน โดยมีเหตุผลรองรับคือเพื่อให้ HR สามารถจัดการระบบการรับส่งพนักงาน เส้นทางการเดินรถ จำนวนรถได้ ซึ่งถือเป็นสวัสดิการอย่างหนึ่งของบริษัท

7. สวัสดิการห้องพยาบาลที่มีแพทย์หรือพยาบาล

ในกรณีที่บริษัทหรือโรงงานขนาดใหญ่มีพยาบาลซึ่งเป็นพนักงานของบริษัทเอง ถือเป็น Data Controller เดียวกัน อาจจะบริหารจัดการได้ง่าย แต่ถ้าใช้แพทย์หรือพยาบาลบุคคลภายนอกหรือ Outsource ถือเป็น Data Processor ในการเก็บข้อมูลส่วนบุคคลด้านสุขภาพ พยาบาลมีความจำเป็นต้องคุ้มครองข้อมูลสุขภาพของพนักงาน ซึ่งถือเป็นข้อมูลส่วนบุคคลละเอียดอ่อน ดังนั้นจึงต้องมีการทำความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้แก่แพทย์และพยาบาลด้วย ในกรณีที่บริษัทมีสวัสดิการมากกว่าสวัสดิการที่กล่าวมาข้างต้น บริษัทจะต้องพิจารณาว่าเข้าข่ายกฎหมายมาตราใด และจะต้องขอความยินยอมหรือดำเนินการอย่างไรเพื่อให้สอดคล้องกับกฎหมายอีกด้วย

8. การฝึกอบรมให้พนักงาน

ในการฝึกอบรม ไม่มีการเก็บข้อมูลส่วนบุคคลละเอียดอ่อน จะใช้เฉพาะข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ นามสกุล ตำแหน่ง เบอร์โทร อีเมล์ เป็นต้น โดยการฝึกอบรมพนักงานสามารถแยกออกเป็น 2 ประเภท คือ การฝึกอบรมในประเทศและการฝึกอบรบต่างประเทศ 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 เพราะอยู่ภายในบริษัท

3) Online Training

การฝึกอบรมออนไลน์ ในปัจจุบันสามารถขึ้นทะเบียนขอรับรองหลักสูตรกับกรมพัฒนาฝีมือแรงงานได้

โดยจะต้องเก็บข้อมูลส่วนบุคคล เช่น ใบหน้า ซึ่งต้องบันทึกภาพการอบรมไว้ตลอดการฝึกอบรม ในการฝึกอบรมแบบออนไลน์นั้น มีเรื่องที่ต้องคำนึงถึง คือ เรื่อง Security บริษัทควรจะต้องรู้ว่าใช้ Provider ของใคร ซึ่งในการเลือกใช้ ควรจะเลือกใช้ที่ได้รับการรับรองว่าได้ขึ้นทะเบียน Security กับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแล้ว ระบบออนไลน์สามารถบันทึกได้ และคุ้มครองข้อมูลส่วนบุคคลได้ รู้ว่า server เก็บไว้ที่ใด มีระบบการคุ้มครองดี และสามารถตรวจสอบได้ ทั้งนี้ในส่วนของการขึ้นทะเบียนรับรองหลักสูตรกับกรมพัฒนาฝีมือแรงงาน กรณีที่มีพนักงาน 100 คนขึ้นไป จะต้องมีการเปิดเผย ชื่อ นามสกุล แผนก และรหัสบัตรประชาชน ของผู้เข้าอบรม ซึ่งเป็นไปตามฐานกฎหมาย เนื่องจากมีพระราชบัญญัติในเรื่องดังกล่าวอยู่แล้ว

การฝึกอบรมต่างประเทศ

ในกรณีที่บริษัทต้องส่งพนักงานเพื่อไปฝึกอบรมที่ต่างประเทศ ไม่ว่าจะเป็น Public Training หรือ In-House Training ที่บริษัทที่เป็นสำนักงานใหญ่ ในส่วนของการคุ้มครองข้อมูลส่วนบุคคล จะเกี่ยวข้องกับ Privacy Notice หรือการแจ้งตามมาตรา 23 โดยใช้ Lawful Basis ตามฐานสัญญาได้ ซึ่งเป็นการส่งข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลส่วนบุคคลทั่วไป

ข้อควรคำนึง คือ ระบบ security ของประเทศปลายทาง ซึ่งควรจะต้องมีระบบ Security ที่ดี มี Data Protection Law ที่เข้มแข็ง และ Implement ได้เหมือนของไทย เพื่อความมั่นใจในการส่งข้อมูลส่วนบุคคลออกไป ทั้งนี้ในการส่งข้อมูลส่วนบุคคลออกไปต่างประเทศ ควรพิจารณาตามมาตรา 28-29 ซึ่งหากมาตราฐานของประเทศปลายทางไม่ดีเพียงพอ บริษัทควรจะต้องแจ้งเจ้าข้อมูลส่วนบุคคลเพื่อขอความยินยอมก่อน ก่อน หรือปฏิบัติตามมาตรา 28-29 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลที่กำหนดให้ บริษัทจะต้องเป็นผู้รับผิดชอบคนแรกหากเกิดปัญหา ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

9. การจ้างแรงงานต่างด้าว กับการเก็บข้อมูลส่วนบุคคล

แรงงานต่างด้าวที่ทำงานในไทยนั้นมีหลายแบบ ทั้งในระดับผู้บริหาร และระดับแรงงาน ที่ส่วนใหญ่จะเป็นแรงงานต่างด้าวตาม MOU คือ พม่า กัมพูชา ลาว ซึ่งไม่ว่าจะมาจากประเทศใดล้วนจำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น ไม่ว่าประเทศนั้น ๆ จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ในฐานะที่บริษัทเป็น Data Controller หรือผู้ควบคุมข้อมูลส่วนบุคคล

ในการเข้ามาทำงานในประเทศไทยนั้นก่อนที่จะเดินทางเข้าประเทศ แรงงานต่างด้าวจะต้องมีการส่งข้อมูลส่วนตัว เช่น ทะเบียนบ้าน สำเนาพาสปอร์ตเพื่อให้บริษัทได้นำไปใช้ในการยื่นเรื่อง เพื่อให้แรงงานต่างด้าวสามารถขอวีซ่าเข้าประเทศ รวมไปถึงการทำ Work Permit ซึ่งหากแรงงานต่างด้าวอยู่ในประเทศไทยเกิน 90 วันก็จะต้องมีการยื่นเรื่องแจ้งกองตรวจคนเข้าเมืองทุก ๆ 90 วัน กระบวนการเหล่านี้ซึ่งล้วนเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งสิ้น

การตรวจสุขภาพแรงงานต่างด้าว

ถึงแม้ว่าจะไม่มีกฎหมายหรือข้อบังคับให้นายจ้างสามารถทำการตรวจสุขภาพก่อนเข้างานได้ ยกเว้นกลุ่มธุรกิจอาหาร ที่พนักงานจะต้องมีการสัมผัสกับอาหาร ตาม พ.ร.บ. สาธารณสุข แต่สำหรับแรงงานต่างด้าว จะสามารถตรวจสุขภาพก่อนเข้างานได้ตาม พ.ร.บ.ตรวจสุขภาพของแรงงานต่างด้าว โดยจะต้องมีใบรับรองแพทย์ 7 โรคด้วยกัน เพื่อใช้ในการยื่นขอ Work Permit ซึ่งในกรณีนี้บริษัทสามารถดำเนินการขอข้อมูลส่วนบุคคลประเภทละเอียดอ่อนได้ตามฐานกฎหมาย โดยไม่ต้องขอความยินยอม

ในการดำเนินการเพื่อให้แรงงานต่างด้าวทำงานในประเทศไทยนั้น HR ต้องเป็นผู้ไปยื่นเอกสารต่าง ๆ กับหน่วยงานราชการหรือจ้าง Outsource เป็นผู้ดำเนินการ ซึ่งจะต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งหมด ถ้าดำเนินการโดยพนักงานของบริษัท ข้อมูลก็จะไหลเวียนอยู่ในองค์กร แต่หากมีการจ้าง outsource บริษัทจำเป็นต้องให้ Outsource ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลด้วย เพราะหาก Outsource ไม่มีความรู้ อาจเกิดละเมิดได้ โดยเฉพาะในกรณีที่แรงงานต่างด้าวมาจากประเทศในกลุ่ม EU หรือสหรัฐอเมริกา ซึ่งให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว โดยในการคัดเลือก Outsource อาจต้องคัดเลือกบริษัทที่มีระบบคุ้มครองข้อมูลส่วนบุคคลที่ถูกต้องและดีพอ ซึ่งจะสามารถตรวจสอบได้ง่ายกว่า การใช้บุคคลธรรมดา ซึ่งอาจจะต้องให้ความรู้เกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ต้องมีการทำ Data Processing Agreement (DPA) อีกด้วย เพราะ Outsource ถือเป็น Data Processor

10. สหภาพแรงงานกับการเก็บข้อมูลส่วนบุคคล

ในบริษัทที่มีสหภาพแรงงาน จะเกี่ยวข้องกับ พรบ.คุ้มครองข้อมูลส่วนบุคคล มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

ซึ่งหากบริษัทมีการสอบถามว่าใครเป็นสมาชิกสหภาพแรงงาน จะเข้าข่ายกฎหมายมาตราดังกล่าว คือ ต้องมีการขอความยินยอม สหภาพแรงงานนั้นถือเป็นอีกนิติบุคคลหนึ่งที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ต้องมี Data Protection Policy ที่เอาไปใช้กับสมาชิกของสหภาพ และหากต้องมีกิจกรรมไหนที่ต้องขอความยินยอมสมาชิกก็จะต้องดำเนินการเช่นกัน ซึ่งบทบาทของบริษัทกับสหภาพแรงงานอาจจะแตกต่างกัน

กรณีศึกษา กิจกรรมหักค่าบำรุงสมาชิก

ใน พ.ร.บ. คุ้มครองแรงงาน ตามมาตรา 76 นั้น นายจ้างสามารถหักค่าบำรุงสมาชิกเพื่อชำระให้แก่สหภาพแรงงานได้ ซึ่งสหภาพแรงงานจะต้องมีข้อตกลงหรือข้อเรียกร้องมายังบริษัทให้ช่วยหักค่าสมาชิกของพนักงานดังรายชื่อที่จัดส่งมาให้ โดยทางสหภาพแรงงานจะต้องเป็นผู้ขอความยินยอมกับสมาชิกโดยตรง เนื่องจากมีบทบาทเป็น Data Controller ของสหภาพ ในขณะที่บริษัทจะทำหน้าที่ในส่วนของ Data Processor คือดำเนินการหักค่าบำรุงสมาชิกตามที่สหภาพแจ้งมาเท่านั้น ไม่สามารถดำเนินการอื่นใดเพิ่มเติมจากข้อตกลงได้

11. กิจกรรมสอบสวนทางวินัย

กรณีที่สหภาพมีข้อเรียกร้อง เช่น ในกรณีที่สมาชิกของสหภาพแรงงานทำผิดระเบียบวินัยและมีการตั้งคณะกรรมาการสอบสวน หนึ่งในคณะกรรมการสอบสวนนั้น จะต้องเป็นคณะกรรมการของสหภาพแรงงานหรือคณะกรรมการลูกจ้าง

หากบริษัทจะมีการลงโทษพนักงาน บริษัทจะต้องแจ้งพนักงานว่าหากเป็นสมาชิกสหภาพฯ ให้ไปแจ้งสหภาพฯ เพื่อให้สหภาพฯ มาแจ้งบริษัท เพื่อเชิญสหภาพฯ มาเป็นคณะกรรมการสอบสวน ไม่ว่าเราจะทราบหรือไม่ว่าพนักงานรายนั้นเป็นสมาชิกของสหภาพฯ หรือไม่ บริษัทจะไม่เป็นผู้ขอความยินยอมเอง แต่จะให้สหภาพฯ ขอความยินยอมแล้วจึงมาแจ้งบริษัท

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

พรบ.แรงงานสัมพันธ์ในมาตรา 13 จะแตกต่างจากมาตรา 15 ดังนี้

มาตรา 13 ลูกจ้างสามารถยื่นข้อเรียกร้องไปที่นายจ้างได้ ในกรณีที่ลูกจ้างไม่ได้เป็นสหภาพฯ โดยมีการรวมตัวกัน 15% ของพนักงาน ระบุรายชื่อ ลายเซ็นต์ ยื่นมาที่บริษัท เพื่อขอเรียกร้อง ในกรณีนี้สามารถทำได้

มาตรา 15 ถ้าเป็นกลุ่มสหภาพแรงงาน ตัวแทนสหภาพแรงงานสามารถยื่นข้อเรียกร้องมาที่บริษัทได้โดยไม่ต้องแสดงรายชื่อสมาชิก ซึ่งหากบริษัทสงสัยว่าจำนวนไม่ครบตามที่กฎหมายกำหนด สามารถทำเรื่องขอเช็ครายชื่อกับสวัสดิการคุ้มครองแรงงาน ซึ่งก็จะไม่เปิดเผยรายชื่อเช่นกัน แต่จะแจ้งว่าครบตามเปอร์เซ็นต์ที่กฎหมายกำหนดหรือไม่

แนวปฏิบัติเกี่ยวกับระยะเวลาในการจัดเก็บข้อมูล

การจัดเก็บข้อมูลและเอกสารส่วนบุคคล เป็นมาตรการที่ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลต้องปฏิบัติตามข้อกำหนดในพรบ. ส่วนเงื่อนไขระยะเวลานั้น เป็นการกำหนดได้เองโดยนโยบายของบริษัทฯ ใช้หลักการและพื้นฐานทางกฎหมายสำหรับเรื่องหรือเอกสารนั้นๆ หรือฐานกฎหมายเฉพาะประเภทธุรกิจที่กำหนดไว้ เช่น ธนาคาร สถาบันการเงิน ประกันภัย เป็นต้น

ข้อกฎหมายสำหรับอายุความในกรณีต่าง ๆ

ประเด็น	อายุ	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

ประเด็น	อายุ	มาตรา
กรณีลูกจ้กรณีนายจ้างใช้สิทธิไล่เบี้ยจากลูกจ้างที่นายจ้างชดใช้ให้แก่บุคคล ภายนอกางฟ้องเรียกค่าจ้าง	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

๑๕. นิติกรระดับชำนาญการขึ้นไป กองนิติการ — คณะทำงาน และผู้ช่วยเลขานุการ

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 ๙ 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 บุญเกิบ 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

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 ๒๑ พฤษภาคม พ.ศ. ๒๕๖๕

(นายนิยม สองแก้ว)
อธิบดีกรมสวัสดิการและคุ้มครองแรงงาน

2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

3. ข้อมูลพระราชบัญญัติคุ้มครองแรงงาน
https://www.krisdika.go.th/librarian/get?sysid=642571&ext=ht-m&fbclid=IwAR2tj_wznFC0g5bmQQy7eT43eImRam-Unb58mswJhtFJZjt-60uDJzPiTQ0

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4. การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565
https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000002400

5. หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565
https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000002600

6. มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000002800

7. หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565
https://ratchakitcha2.soc.go.th/pdfdownload/?id=139D140S0000000003200

8. ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. 2565
http://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/165/T_0001.PDF

สนับสนุนโดย


SME
สมาพันธ์เอสเอ็มอีไทย


PDPA
THAILAND


DIGITAL BUSINESS CONSULT CO., LTD.


dcti