EU รับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่น กรณีศึกษาสำหรับประเทศไทย

By **thaieurope** - September 19, 2018

EU เริ่มกระบวนการให้การรับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่น (Adequacy Decision) เพื่ออำนวยความสะดวกในการรับ-ส่งข้อมูลระหว่างประเทศสมาชิก EU และญี่ปุ่น หลังจากที่ EU เห็นชอบในเนื้อหาการรับรองมาตรฐานการคุ้มครองมาตรฐานของญี่ปุ่นไปเมื่อเดือนกรกฎาคม 2561 ล่าสุดเมื่อวันที่ 5 กันยายน 2561 EU ได้เริ่มกระบวนการให้การรับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่น ภายใต้กฎระเบียบ GDPR ที่มีผลบังคับใช้ไปตั้งแต่เดือนพฤษภาคม 2561 ที่ผ่านมา

ภาคธุรกิจของญี่ปุ่นต้องเพิ่มความเข้มงวดด้านการคุ้มครองข้อมูลส่วนบุคคลเพิ่มมากขึ้น เพราะร่างข้อมติรับรองมาตรฐานการคุ้มครองข้อมูล (Draft Decision) ที่จัดทำโดยคณะกรรมาธิการยุโรป ระบุข้อปฏิบัติเพิ่มเติม (Supplementary Rules) จากกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นที่มีอยู่แล้ว (Act on the Protection of Personal Information : APPI) โดยข้อปฏิบัติเพิ่มเติมดังกล่าว มีสาระสำคัญ ดังต่อไปนี้

1. **กระบวนการทำให้ข้อมูลยืนยันตัวบุคคลไม่ปรากฏชื่อของบุคคลนั้น หรือสิ่งที่สามารถระบุตัวตนของบุคคลนั้น (anonymization)** โดยจะต้องไม่ให้สามารถระบุตัวตนได้อีก เพื่อปกป้องข้อมูลส่วนบุคคลที่ได้รับการโอนมาจากประเทศสมาชิก EU ซึ่งภาคธุรกิจของญี่ปุ่นจะต้องลบข้อมูลสำคัญที่จะทำให้สามารถระบุตัวตนได้ ([…] destroy the key permitting to re-identify the data) ทั้งนี้ เพราะกฎหมาย APPI ของญี่ปุ่น ระบุเพียงแค่ให้มีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้เท่านั้น ([…] merely required to prevent re-identification) แต่อาจใช้วิธีการอื่นๆ เพื่อระบุตัวตนได้
2. **ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครองโดยเจ้าของข้อมูลเท่ากันที่มีสิทธิ** เช่น สิทธิในการเข้าถึงเพื่อตรวจสอบ สิทธิในการแก้ไขข้อมูล หรือการไม่ยินยอมให้ประมวลผล เป็นต้น ซึ่งรวมถึงข้อมูลที่มีกำหนดลบทิ้ง (set to be deleted) ภายในระยะเวลาไม่เกิน 1 ปี เนื่องจากกฎหมาย APPI ไม่ได้ให้สิทธิการคุ้มครองข้อมูลประเภทดังกล่าว
3. **การนำข้อมูลไปประมวลผลไม่สามารถใช้เกินขอบเขตที่เจ้าของข้อมูลให้ความยินยอมไว้** โดยจะต้องขอความยิมยอมใหม่ทุกครั้ง ซึ่งต่างจากกฎหมาย APPI เดิมที่ไม่มีความชัดเจนเกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูล ในกรณีที่จุดประสงค์ในการประมวลผลข้อมูลแตกต่างไปจากจุดประสงค์เดิมที่เจ้าของข้อมูลให้ความยินยอมไว้ก่อน
4. **การยกระดับการคุ้มครองข้อมูลละเอียดอ่อน (sensitive data) ภายใต้กฎระเบียบ GDPR ให้ได้รับการคุ้มครองแบบพิเศษ (special care-required personal information) ตามกฎหมาย APPI** เพราะข้อมูลประเภทข้อมูลละเอียดอ่อนภายใต้กฎระเบียบ GDPR เช่น เชื้อชาติ ศาสนา ประวัติการรักษา และอาชญากรรม เป็นประเภทข้อมูลเดียวกันกับข้อมูลประเภทที่ได้รับการคุ้มครองพิเศษ ภายใต้กฎหมาย APPI
5. **การโอนข้อมูลส่วนบุคคลของผู้ที่มีถิ่นพำนักใน EU จากญี่ปุ่นไปยังประเทศที่สาม (onward transfer) จะต้องเป็นไปตามระเบียบที่กำหนดไว้** โดยการโอนข้อมูลส่วนบุคคลต่อจากญี่ปุ่นไปยังประเทศที่สามมี 2 กรณี คือ 1) ประเทศที่สามนั้นได้รับการรับรองมาตรฐานการคุ้มครองข้อมูลจากญี่ปุ่น และ 2) ในกรณีที่ผู้รับโอนอยู่ในประเทศที่มีระดับการให้ความคุ้มครองแตกต่างกัน ผู้ประกอบการต้องจัดทำกฎข้อบังคับหรือสัญญาที่ให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) ตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นและข้อปฏิบัติเพิ่มเติม (Supplementary Rules) ตามที่ญี่ปุ่นมีความตกลงร่วมกับ EU
6. **การใช้ข้อมูลส่วนบุคคลเพื่อทำการตลาดทางตรง (Direct Marketing) จะต้องได้รับการยินยอมจากเจ้าของข้อมูล และต้องสามารถให้เจ้าของข้อมูลบอกยกเลิกการใช้ข้อมูลส่วนบุคคลได้ (opt-out)** โดยการใช้ข้อมูลส่วนบุคคลที่โอนจาก EU ไปยังญี่ปุ่น หรือจากญี่ปุ่นไปยังประเทศที่สามจะต้องเป็นไปตามจุดประสงค์เดิมที่เจ้าของข้อมูลได้ให้ความยินยอมไว้เท่านั้น หากต้องการใช้ข้อมูลเพื่อทำการตลาดทางตรงเพิ่มเติม จะต้องขอความยินยอมจากเจ้าของข้อมูลก่อน รวมทั้งต้องให้เจ้าของข้อมูลสามารถบอกยกเลิกการใช้ข้อมูลของตนได้ทุกเมื่อ (opt-out)
7. **การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความเข้มงวดมากขึ้น โดยเฉพาะในกรณีละเมิดการประมวลผลข้อมูลที่โอนจาก EU มายังญี่ปุ่น** ซึ่งผู้ประกอบการจะต้องปฏิบัติตามคำแนะนำของหน่วยงานคุ้มครองข้อมูล และไม่สามารถอ้างเหตุผลใดๆ ที่จะไม่ปฏิบัติตามได้ ยกเว้นกรณีภัยธรรมชาติ หรือผู้ประกอบการได้ปรับปรุงแก้ไขด้วยวิธีการอื่นแล้วเท่านั้น

นอกจากนี้ ญี่ปุ่นยังได้จัดทำมาตรการป้องกันเพิ่มเติมสำหรับการใช้ข้อมูลส่วนบุคคลที่โอนมาจาก EU โดยหน่วยงานภาครัฐ ซึ่งรวมถึงการปฏิบัติงานของตำรวจ และหน่วยงานด้านความมั่นคงอื่นๆ โดยจำกัดการเข้าถึงและการใช้ข้อมูลโดยหน่วยงานภาครัฐ ตามความจำเป็นและสมเหตุสมผล (necessary and proportionate) เท่านั้น โดยเจ้าของข้อมูลใน EU สามารถฟ้องร้องหน่วยภาครัฐได้หากพบกรณีละเมิด

ทั้งนี้ หน่วยงาน European Data Protection Board (EDPB) จะต้องให้ความเห็นต่อร่างข้อมติรับรองมาตรฐานการคุ้มครองข้อมูล (Draft Decision) ก่อน จากนั้นจะต้องขอความเห็นชอบจากประเทศสมาชิก และรายงานต่อไปยังคณะกรรมการด้าน Civil Liberties, Justice and Home Affairs ของสภายุโรป เพื่อให้คณะกรรมาธิการยุโรปเต็มคณะ (College of Commission) ให้การรับรอง โดยคาดว่า กระบวนการการรับรองมาตรฐานการคุ้มครองข้อมูลจะเสร็จสิ้นภายในปี 2562

ประเด็นที่เป็นกรณีศึกษาที่สำคัญสำหรับประเทศไทย

ข้อมูลส่วนบุคคลเป็นปัจจัยสำคัญในการประกอบธุรกิจในปัจจุบัน ที่เน้นการเชื่อมโยงเข้ากับเศรษฐกิจโลกมากยิ่งขึ้น ซึ่งอาจส่งผลให้เกิดการละเมิดการใช้ข้อมูลส่วนบุคคลและก่อให้เกิดความเสียหายได้ ในหลายประเทศจึงมีข้อจำกัดในการโอนข้อมูลส่วนบุคคลออกนอกประเทศที่มีระดับการคุ้มครองข้อมูลแตกต่างกัน โดยในปัจจุบัน ประเทศไทยอยู่ระหว่างการจัดทำ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อพัฒนานโยบายและกฎระเบียบต่างๆ ที่เกี่ยวข้องให้สอดคล้องกับความก้าวหน้าของเทคโนโลยีสารสนเทศ และแนวปฏิบัติที่เป็นสากล

การรับรองมาตรฐานการคุ้มครองข้อมูลระหว่างอียูกับญี่ปุ่นในครั้งนี้ ส่งผลให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นมีระดับสูงขึ้น การโอนข้อมูลส่วนบุคคลไปยังประเทศที่มีมาตรฐานต่ำกว่าจึงมีข้อจำกัด ซึ่งหลังจากการผนวกรวมข้อปฏิบัติเพิ่มเติม (Supplementary Rules) ข้างต้น ก็น่าจะเรียกได้ว่า ญี่ปุ่นมีระดับมาตรฐานการคุ้มครองข้อมูลสูงที่สุดเลยก็ว่าได้ ซึ่งนั่นก็หมายความว่า การโอนข้อมูลจากญี่ปุ่น โดยเฉพาะการส่งต่อข้อมูลจาก EU (onward transfer) ไปยังประเทศที่สามจะไม่สามารถทำได้ หากประเทศนั้นไม่ได้รับการ

รับรองมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ ซึ่งในฐานะที่ญี่ปุ่นเป็นทั้งคู่ค้าและนักลงทุนที่สำคัญอันดับต้นๆ ของไทย การโอนข้อมูลระหว่างหน่วยธุรกิจถือเป็นปัจจัยสำคัญ ประเทศไทยจึงต้องให้ความสำคัญกับการพัฒนามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก

ทั้งนี้ เป็นที่สังเกตว่า EU มองว่า แนวทางการคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดนตามกรอบของ APEC (APEC Cross-Border Privacy Rules System) ยังไม่เพียงพอ โดยในร่างข้อมติรับรองมาตรฐานการคุ้มครองข้อมูล (Draft Decision) ที่จัดทำโดยคณะกรรมาธิการยุโรป ได้ระบุเกี่ยวกับแนวทางการคุ้มครองข้อมูลส่วนบุคคลในกรอบ APEC ว่า ไม่ได้เกิดจากความตกลงระหว่างผู้ส่งออกข้อมูล (exporter) และผู้นำเข้าข้อมูล (importer) อีกทั้ง ยังถือว่ามีมาตรฐานการคุ้มครองที่ต่ำกว่ามาตรฐานของญี่ปุ่นและข้อปฏิบัติเพิ่มเติม (Supplementary Rules)

การยกระดับมาตรฐานการคุ้มครองข้อมูลของไทยให้สอดคล้องกับกฎระเบียบ GDPR อาจหลีกเลี่ยงไม่ได้ เพื่ออำนวยความสะดวกให้แก่องค์กรในภาคธุรกิจที่รวดเร็วและประหยัด โดยเฉพาะในปัจจุบันที่รูปแบบการดำเนินธุรกิจต้องสามารถเชื่อมโยงกันได้ แทนที่ผู้ประกอบการจะต้องเสียเวลาและค่าดำเนินการเพื่อจัดทำกฎข้อบังคับหรือสัญญาที่ให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) หรือสัญญามาตรฐาน (Model Contracts) เพื่อโอนข้อมูลไปยังประเทศที่มีระดับการให้ความคุ้มครองแตกต่างกัน เป็นต้น นอกจากนี้ สาระสำคัญของการรับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่นยัง**ครอบคลุมแนวปฏิบัติของทั้งหน่วยงานภาครัฐและองค์กรในภาคธุรกิจ** ซึ่งแตกต่างจากการรับรองมาตรฐานการคุ้มครองข้อมูลของแคนาดาและสหรัฐฯ ที่ครอบคลุมแนวปฏิบัติเฉพาะองค์กรในภาคธุรกิจเท่านั้น โดยก[illegible] ครอบคลุมเฉพาะองค์กรในภาคธุรกิจที่ปฏิบัติตามแนวทางภายใต้กรอบตามความตกลง Privacy Shield เท่านั้น ซึ่งไทยสามาร[illegible] เสียของการจัดทำมาตรฐานการคุ้มครองข้อมูลของไทยให้เทียบเท่าประเทศคู่ค้าเหล่านี้ รวมถึงข้อดีข้อเสียของรูปแบบการรับร[illegible] แต่ละประเทศ เพื่อสนับสนุนเป้าหมายการเป็นผู้นำเศรษฐกิจดิจิตัลของไทยในอนาคต

อ่านเพิ่มเติมเกี่ยวกับ Draft Decision ได้ ที่นี่

สนับสนุนโดยงบประมาณของกระทรวงการต่างประเทศ ข้อมูลจากทีมประเทศไทย ณ กรุงบรัสเซลส์
และส่วนราชการไทยทุกแห่งในยุโรป