GDPR: GENERAL DATA PROTECTION REGULATION

SUMMARY

GDPR หรือ General data protection regulation นั้นเป็น กฎของสหภาพยุโรป (EU) เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของพลเมือง EU ซึ่งมีผลใช้บังคับเมื่อวันที่ 25 พฤษภาคม พ.ศ. 2561 ที่ผ่านมา

ขอบเขตของการบังคับใช้
GDPR ใช้กับองค์กรต่าง ๆ ที่ได้มีการประมวลผลข้อมูลส่วนบุคคลของพลเมืองใน EU ไม่ว่าจะเป็นองค์กรใน EU หรือองค์กรที่ไม่ได้อยู่ใน EU แต่ได้มีการจำหน่ายสินค้าและบริการให้แก่พลเมืองของ EU ด้วย

การขอความยินยอม
การขอความยินยอมที่อยู่ภายใต้ GDPR นั้นจะต้องมีความชัดแจ้งในวัตถุประสงค์ของการขอความยินยอม รูปแบบการขอความยินยอมต้องมีความชัดเจน ใช้ภาษาที่เข้าใจง่าย และจะต้องจัดให้มีวิธีการในการถอนความยินยอมที่ง่ายด้วย

สิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล

1.สิทธิในการได้รับแจ้งเมื่อเกิดการรั่วไหลของข้อมูล(Breach and notification)

หากข้อมูลส่วนบุคคลมีการรั่วไหล และการรั่วไหลนั้นอาจมีผลเสี่ยงต่อสิทธิ/เสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ที่จะต้องแจ้งต่อหน่วยงานกำกับดูแล ภายใน 72 ชั่วโมง นับแต่รู้ถึงการรั่วไหล ซึ่งหากฝ่าฝืนอาจมีโทษปรับ

2.สิทธิในการที่จะได้รับข้อมูลของตนเองไปใช้ในบริการต่าง ๆ (Data portability)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับข้อมูลส่วนบุคคลที่เกี่ยวกับตน เพื่อเคลื่อนย้าย คัดสำเนา หรือ ถ่ายโอนข้อมูลส่วนบุคคล ไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น ได้โดยง่าย

3.สิทธิในการที่จะเข้าถึงข้อมูล (Right to access)

เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบความถูกต้องของการประมวลผลข้อมูลส่วนบุคคลได้ GDPR ได้กำหนดให้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการแจ้งวิธีการประมวลผลข้อมูล รวมทั้งมีสิทธิได้รับการแจ้งว่าะมีการนำข้อมูลไปใช้เพื่อวัตถุประสงค์ใดซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ที่จะต้องจัดทำข้อมูลเป็นสำเนาอิเล็กทรอนิกส์ ให้เจ้าของข้อมูล โดยไม่คิดค่าใช้จ่ายใด ๆ

4.สิทธิที่จะได้รับการคุ้มครองจากการการออกแบบระบบเพื่อคุ้มครองข้อมูลส่วนบุคคล (Privacy by designed)

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องออกแบบและสร้างระบบ รวมถึงมีมาตรการทางเทคนิคอื่น ๆ ที่เหมาะสม เพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ของ GDPR และปกป้องสิทธิของเจ้าของข้อมูลอย่างมีประสิทธิภาพ

5. สิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตนออก (Right to be forgotten)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลส่วนบุคคลของตนออก โดยการขอให้ลบข้อมูลนั้นอยู่ภายใต้เงื่อนไขต่าง ๆ เช่น การเก็บข้อมูลนั้นไม่เป็นไปตามวัตถุประสงค์เดิมอีกต่อไป เป็นต้น

6. สิทธิที่จะได้รับความคุ้มครองจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนุคคล (Data protection officers)

ผู้ประมวลผลข้อมูลและผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO หรือ data protection officers) หากองค์กรนั้นมีลักษณะตามที่ GDPR กำหนด โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ติดตามการประมวลผลข้อมูล และให้คำแนะนำในการปฏิบัติตาม GDPR

บทกำหนดโทษ

ในกรณีที่องค์กรไม่ปฏิบัติให้เป็นไปตามที่ GDPR กำหนด อาจถูกปรับได้ถึง 20 ล้านยูโร หรือ ร้อยละ 4 ของรายได้ทั่วโลก (ขึ้นอยู่กับว่าจำนวนใดจะสูงกว่า)

ผลกระทบต่อประเทศไทย

เนื่องจาก GDPR นั้น นำไปใช้กับองค์กรธุรกิจที่อยู่ภายใน EU และภายนอก EU ด้วย ดังนั้น GDPR อาจมีผลกระทบต่อผู้ประกอบกิจการของประเทศไทย ในกรณีที่เป็นการประกอบกิจการที่มีการจำหน่ายสินค้าหรือบริการให้กับ พลเมือง EU ซึ่งได้มีการประมวลผลข้อมูลส่วนบุคคลของพลเมือง EU

นางสาวกนกอร ฟองศา นิติกร
สำนักกฎหมาย สำนักงานเศรษฐกิจการคลัง