GDPR คืออะไร สำคัญอย่างไร?
ทำไมจึงต้องเข้าใจ GDPR ?

นคร เสรีรักษ์
- ผู้ช่วยศาสตราจารย์, วิทยาลัยการปกครองท้องถิ่น มหาวิทยาลัยขอนแก่น
- ผู้ก่อตั้ง PrivacyThailand
- กรรมการผู้ทรงคุณวุฒิ คณะกรรมการข้อมูลข่าวสารของราชการ

ความสนใจหรือความตระหนักรู้เรื่องความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนับว่ามีอยู่ค่อนข้างน้อย โดยเฉพาะในโลกปัจจุบันที่คนไทยนิยมใช้โซเชียลมีเดียกันจนติดอันดับต้นๆ ของโลก เราโพสต์เราแชร์ข้อมูลส่วนตัวบนโลกออนไลน์โดยไม่เคยตระหนักถึงความสำคัญของความเป็นส่วนตัว ที่น่าห่วงกว่าการไม่เห็นคุณค่าในพื้นที่ส่วนตัว คือการไม่ตระหนักถึงอันตรายหรือความเสียหายที่จะเกิดจากการโจรกรรมข้อมูลของเราไปใช้ประโยชน์ในทางไม่ชอบ จนพูดกันว่าความเป็นส่วนตัวตายไปแล้วจากโลกดิจิทัลวันนี้

ระยะหลังนี้ เริ่มมีการพูดถึงข้อมูลส่วนบุคคลกันมากขึ้น โดยเฉพาะในแวดวงผู้ประกอบธุรกิจเกี่ยวกับข้อมูล การติดต่อสื่อสาร และธุรกิจที่มีฐานข้อมูลส่วนบุคคลขนาดใหญ่ นั่นคือผลที่เกิดจาก **ความกังวลต่อ GDPR ซึ่งเป็นข้อบังคับของสหภาพยุโรปเกี่ยวกับการเก็บและการประมวลผลข้อมูลส่วนบุคคล เหตุที่กลัวกันมากก็เพราะบทลงโทษของผู้ที่ไม่ปฏิบัติตามหลักเกณฑ์ GDPR จะถูกปรับสูงถึง 20 ล้านยูโร ที่สำคัญคือมีผลบังคับใช้แล้วตั้งแต่เดือนพฤษภาคม 2561 ที่ผ่านมา**

แท้จริงแล้วการคุ้มครองข้อมูลส่วนบุคคลในระดับนานาชาติไม่ใช่เรื่องใหม่ เพราะมีพัฒนาการมากมายทั้งในกฎหมายต่างประเทศในนานาประเทศและกฎหมายหรือข้อตกลงระหว่างประเทศในหลายเวที เช่น การคุ้มครองข้อมูลตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน แนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ข้อตกลงของรัฐสภาแห่งยุโรป ข้อบังคับสหภาพยุโรป (European Union Directive 95/46/EC) แนวทางของสหประชาชาติ การคุ้มครองข้อมูลตามแนวทางของ APEC, ASEAN และ TPP

การคุ้มครองข้อมูลส่วนบุคคลตามข้อบังคับ EU

การคุ้มครองข้อมูลส่วนบุคคลตาม EU Directive 95/46 เกิดขึ้นในปี 1995 เป็นบทบัญญัติที่มีผลบังคับระหว่างประเทศฉบับแรกที่ให้ความคุ้มครองข้อมูลส่วนบุคคล ข้อบังคับนี้สร้างขึ้นโดยประเทศสมาชิกสหภาพยุโรปเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล ทั้งยังให้การรับรองว่าข้อมูลจะได้รับการคุ้มครองอย่างเท่าเทียมกันตลอดทั้งตลาดร่วมยุโรป โดยมีหลักการที่เป็นสาระสำคัญดังนี้

1. การรักษาคุณภาพของข้อมูล
2. มาตรการของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย
3. ข้อกำหนดในการประมวลผลข้อมูลพิเศษ/ข้อมูลที่อ่อนไหว (sensitive data)
4. สิทธิในการได้รับแจ้งการเก็บข้อมูลต่างๆ
5. สิทธิในการเข้าถึงข้อมูล
6. สิทธิในการคัดค้านการประมวลผล
7. การรักษาความปลอดภัยในการประมวลผลข้อมูล
8. การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม

นอกจากการควบคุมการส่งข้อมูลภายในประเทศสมาชิกแล้ว หากประเทศที่ไม่ได้เป็นสมาชิกสหภาพยุโรปจะติดต่อรับ-ส่งข้อมูลกับประเทศสมาชิกสหภาพยุโรป ก็ต้องมีมาตรการการคุ้มครองข้อมูลที่เหมาะสมเป็นที่พอใจแก่สหภาพยุโรปด้วยเช่นกัน มาตรการที่เหมาะสมตามที่ EU ได้ตั้งไว้นี้ แม้กระทั่งประเทศสหรัฐอเมริกาที่มีการค้าและการลงทุนกับประเทศสมาชิกสหภาพยุโรปมากที่สุดและมีการเคลื่อนไหวของข้อมูลข่าวสารมากที่สุด ก็ยังต้องพยายามหาวิธีการประนีประนอมเพื่อหาทางออกและแก้ไขปัญหาความขัดแย้งของทั้งสองฝ่าย

EU Directive 95/46 ใช้บังคับมานานกว่า 20 ปี และโดยที่โลกเปลี่ยนแปลงไปอย่างมากในปัจจุบัน โดยเฉพาะบริบทการสื่อสารผ่านทางอิเล็กทรอนิกส์ได้เติบโตพัฒนาอย่างรวดเร็วมาก จึงเกิดการปรับปรุงแก้ไข Directive ดังกล่าว กระทั่งในที่สุดรัฐสภาแห่งยุโรปก็ได้เห็นชอบ General Data Protection Regulation (GDPR) เมื่อ 14 เมษายน 2559 และจะมีผลบังคับใช้ในวันที่ 25 พฤษภาคม 2561

GDPR (General Data Protection Regulation)

GDPR เป็นกฎระเบียบของ EU ที่ออกมาเพื่อคุ้มครองประชาชนในกลุ่มประเทศ EU จากการที่ความเป็นส่วนตัวและข้อมูลส่วนบุคคลถูกล่วงละเมิดมากขึ้นในโลกยุคใหม่ที่ขับเคลื่อนด้วยข้อมูลเป็นการปรับปรุงมาตรการให้เหมาะสมกับสถานการณ์ที่แตกต่างไปจากเมื่อครั้งออกกฎ EU Directive เมื่อปี 1995

ความเปลี่ยนแปลงจากข้อกำหนดใน GDPR ที่สำคัญและได้รับความสนใจ หรือตระหนกตกใจกันมาก น่าจะเป็นบทลงโทษที่ระบุไว้ว่า การเก็บและประมวลผลข้อมูลส่วนบุคคลของประชาชน EU ที่ไม่ปฏิบัติตาม GDPR จะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีทั่วโลก ขึ้นอยู่กับว่าวงเงินใดมากกว่า กฎระเบียบนี้มีผลใช้บังคับกับหน่วยงานที่อยู่ใน EU และรวมไปถึงหน่วยงานนอก EU

หลักการคุ้มครองข้อมูลยังคงเป็นไปตามมาตรฐานของ EU Directive โดยมีความเปลี่ยนแปลงที่สำคัญจากข้อกำหนดใน GDPR ดังนี้

1. ขอบเขตการบังคับใช้เชิงพื้นที่

GDPR บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ใน EU ไม่ว่าบริษัทจะตั้งอยู่ที่ไหนในโลก นั่นคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลใน EU ไม่ว่าการประมวลผลจะทำใน EU หรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการ

แก่พลเมือง EU และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นใน EU หากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิก EU (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนใน EU ด้วย

2. บทลงโทษ

ในกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่นกรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบ การไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำ Privacy Impact Assessment

3. การให้ความยินยอม

หลักความยินยอมได้รับการยืนยันเข้มแข็งมากขึ้น โดยระบุว่าการขอความยินยอมต้องดำเนินการในรูปแบบที่เข้าใจได้และสามารถเข้าถึงได้สะดวก (Intelligible and Easily Access) ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอคำยินยอม โดยการขอความยินยอมต้องมีความชัดเจน ใช้ภาษาเข้าใจง่าย นอกจากนี้การยกเลิกการให้ความยินยอมต้องก็ต้องดำเนินการได้ด้วยความสะดวก

สิทธิของเจ้าของข้อมูลภายใต้ GDPR

สิทธิที่จะได้รับแจ้งเมื่อเกิดความเสียหาย (Breach Notification)

ภายใต้ GDPR ถือว่าการแจ้งเป็นหน้าที่ที่ต้องปฏิบัติ เมื่อเกิดความเสียหายหรือการรั่วไหลของข้อมูลซึ่งเกิดผลกระทบมีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ทั้งนี้การแจ้งต้องดำเนินการภายใน 72 ชั่วโมง โดยผู้ประมวลผลต้องแจ้งต่อลูกค้าและผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากเกิดความเสียหาย

สิทธิที่จะรู้และเข้าถึงข้อมูล (Right to Access)

เจ้าของข้อมูลมีสิทธิที่จะได้รับแจ้งจากผู้ควบคุมข้อมูลว่า มีการประมวลผลข้อมูลหรือไม่ การประมวลผลดำเนินการที่ไหน มีวัตถุประสงค์อะไร และเมื่อร้องขอ ผู้ควบคุมข้อมูลจะต้องจัดหาสำเนาข้อมูลดังกล่าวให้เจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยไม่คิดค่าใช้จ่าย

ข้อกำหนดนี้เป็นการเปลี่ยนแปลงที่สำคัญในเรื่องความโปร่งใสของข้อมูลและเป็นการยืนยันความเข้มแข็งของเจ้าของข้อมูล

สิทธิที่จะขอให้ลบข้อมูล (Right to be Forgotten/Right to Erase)

เจ้าของข้อมูลมีสิทธิ (1) ในการแจ้งให้ลบข้อมูล ระงับการเผยแพร่ หยุดการประมวลผลโดยบุคคลที่สาม (2) มีสิทธิในการแจ้งให้ลบข้อมูลที่ไม่มีส่วนเกี่ยวข้องตามวัตถุประสงค์ในการจัดเก็บครั้งแรก และ (3) มีสิทธิในการลบข้อมูลที่เจ้าของข้อมูลได้ยกเลิกความยินยอม

ทั้งนี้ผู้ควบคุมต้องใช้ดุลพินิจในการพิจารณาเปรียบเทียบสิทธิของเจ้าของข้อมูลกับประโยชน์สาธารณะในการมีอยู่ของข้อมูลนั้น

สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง (Data Portability)

สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเองในรูปแบบที่ใช้งานได้ตามปกติรวมทั้งรูปแบบที่อ่านได้ด้วยเครื่องมือ/อุปกรณ์ (machine-readable format)

สิทธิที่จะได้รับความคุ้มครองตั้งแต่ต้น (Privacy by Design/Privacy by Default)

กำหนดให้มีการวางระบบความคุ้มครอง (Protection) ตั้งแต่ในโอกาสแรกของการออกแบบระบบ มากกว่าการมาเพิ่มการดำเนินการในภายหลัง โดยกำหนดว่าต้องมีการใช้มาตรการทางเทคนิคและการบริหารที่เหมาะสม มุ่งยึดหลักประสิทธิภาพ เพื่อให้เป็นไปตามข้อกำหนดและเป็นการคุ้มครองสิทธิเจ้าของข้อมูล

ผู้ควบคุมข้อมูลจะเก็บและและประมวลผลข้อมูลได้เพียงเท่าที่จำเป็นเพื่อให้ภารกิจสำเร็จ (Data Minimization) และต้องจำกัดการเข้าถึงข้อมูลโดยผู้ที่ไม่มีความเกี่ยวข้องใดๆ กับการประมวลผล

สิทธิที่จะได้รับการคุ้มครองโดยเจ้าหน้าที่รับผิดชอบ (Data Protection Officers: DPO)

ใช้ระบบการเก็บบันทึกข้อมูลภายในองค์กร (Internal Record Keeping) แทนระบบการรายงานต่อ Data Protection Authorities (DPA) และกำหนดให้มีการแต่งตั้ง DPO สำหรับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลขนาดใหญ่ และมีภารกิจหลักในการติดตามและประมวลผลข้อมูลเป็นประจำและเป็นระบบ (Regularly and Systematic Monitoring Data Subjects)

การแต่งตั้ง DPO ต้องคำนึงถึงคุณสมบัติด้านวิชาชีพและความเชี่ยวชาญด้านกฎหมายและภาคปฏิบัติการ อาจแต่งตั้งเจ้าหน้าที่ภายในองค์กรหรือผู้ให้บริการภายนอก ต้องแจ้งข้อมูลการติดต่อกับทาง DPA และต้องมีทรัพยากรเหมาะสมกับการปฏิบัติภารกิจและพัฒนาความรู้ความเชี่ยวชาญของ DPO ทั้งนี้ DPO มีระบบรายงานต่อผู้บริหารระดับสูงและต้องไม่ทำหน้าที่อื่นที่อาจเป็นกรณีผลประโยชน์ทับซ้อน

GDPR กับกฎหมายข้อมูลส่วนบุคคลของไทย

ความพยายามในการออกกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีจุดเริ่มต้นในปี 2540 ตลอดหลายปีที่ผ่านมา มีการจัดทำร่างกฎหมายถึง 5 ฉบับ ผ่านรัฐบาลหลายคณะ

จนล่าสุด คณะรัฐประหารในนามคณะรักษาความสงบแห่งชาติ (คสช.) ประกาศจะเร่งออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพราะเห็นว่าเป็นกฎหมายสำคัญที่มีความจำเป็นเร่งด่วนต่อกระบวนการปฏิรูปประเทศ

รัฐบาลปัจจุบันได้ส่งร่างกฎหมายไปยังสภานิติบัญญัติแห่งชาติเมื่อเดือนตุลาคม 2557 หลังจากนั้นไม่ถึงสามเดือน สังคมไทยถูกทำให้สับสนมากขึ้นด้วยการที่รัฐบาลชุดเดียวกันได้เสนอร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกฉบับ ในชุดกฎหมายขับเคลื่อนนโยบายเศรษฐกิจดิจิทัล

ร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ดังกล่าว ได้มีการปรับแก้หลายครั้งจนกลายเป็นร่างล่าสุด ซึ่งผ่านความเห็นชอบของสภานิติบัญญัติแห่งชาติเมื่อวันที่ 28 กุมภาพันธ์ 2562 ที่ผ่านมา

ประเด็นที่ต้องดูกันต่อไปคือ การคุ้มครองข้อมูลส่วนบุคคลตามร่างนี้จะมีมาตรฐานในระดับที่ทาง EU จะยอมรับหรือไม่ ซึ่งเมื่อพิจารณาแล้ว**ประเด็นการส่งข้อมูลข้ามแดนจะเป็นเรื่องสำคัญที่สุด** เพราะการส่งข้อมูลของคนต่างชาติตามมาตรฐานสากลและข้อตกลงระหว่างประเทศจะห้ามส่งข้อมูลไปยังประเทศที่ไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่ต่ำกว่ามาตรฐานของประเทศผู้ส่ง ร่างนี้เขียนว่าการส่งข้อมูลข้าม

แดนให้เป็นไปตามหลักเกณฑ์ที่กรรมการกำหนด โดยที่ในวันนี้ประเทศไทยยังไม่มีกรรมการที่จะดูแลบริหารกฎหมายนี้ จึงยังไม่รู้ว่าหลักเกณฑ์ที่จะออกมาจะมีหน้าตาเป็นอย่างไร ในระหว่างที่ยังไม่มีหลักเกณฑ์ที่ว่าถ้าเกิดกรณีการแลกเปลี่ยน การรับ-ส่งข้อมูลระหว่างไทยกับประเทศสมาชิก EU ทางยุโรปจะเห็นว่ามาตรฐานของไทยภายใต้ร่างนี้จะเทียบเท่า GDPR หรือเปล่า

GDPR กับประเทศไทย

ประเทศไทยคงหลีกเลี่ยงมาตรการ GDPR ได้ยาก เพราะการค้าระหว่างประเทศมีมูลค่าทางเศรษฐกิจสูงมาก และในการดำเนินธุรกิจซึ่งทั้งหมดดำเนินการบนระบบอิเล็กทรอนิกส์ย่อมมีการแลกเปลี่ยนข้อมูลระหว่างผู้ประกอบการตลอดเวลา ปริมาณการรับ-ส่งข้อมูลมีมหาศาล ในบรรดาข้อมูลเหล่านี้ย่อมรวมถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องจำนวนมาก ทั้งข้อมูลพลเมืองของประเทศผู้ซื้อและประเทศผู้ขายสินค้าและบริการ

พิจารณาจากภาคท่องเที่ยวและบริการเพียงส่วนเดียว นักท่องเที่ยวจากยุโรปก็เป็นกลุ่มใหญ่ที่สุดที่ทำรายได้ให้กับภาคการท่องเที่ยวของไทย แน่นอนว่าข้อมูลส่วนบุคคลของนักท่องเที่ยวเหล่านี้จะต้องมีการรับ-ส่ง-แลกเปลี่ยนกับผู้ให้บริการในประเทศไทยอย่างหลีกเลี่ยงไม่ได้

บริษัทและหน่วยงานในประเทศเราจึงน่าจะมีผลกระทบจากกฎระเบียบ GDPR จำนวนมาก ตั้งแต่การเก็บข้อมูลการเดินทางเข้าออกประเทศ ธุรกิจสายการบิน บริษัทท่องเที่ยว โรงแรมที่พัก โรงพยาบาลหรือสถานบริการสุขภาพ สถาบันการเงิน ธุรกิจการเงิน การแลกเปลี่ยนเงินตรา บัตรเครดิต การประกันชีวิต การประกันภัย บริษัทโทรคมนาคม บริษัทที่ดำเนินธุรกิจธุรกรรมออนไลน์ และ E-commerce ทั้งหมด

ฐานข้อมูลส่วนบุคคลในผู้ประกอบการด้านการเงินการธนาคาร ธุรกิจการติดต่อสื่อสารโทรคมนาคม และโดยเฉพาะธุรกิจที่เกี่ยวข้องกับข้อมูลโดยตรง ไม่ว่าจะเป็นผู้ประกอบการด้านการประมวลผลข้อมูล Big Data Cloud รวมทั้งธุรกิจตลาดหลักทรัพย์ ธุรกิจบริการด้านสุขภาพ ล้วนจัดเก็บข้อมูลปริมาณมหาศาล ทุกหน่วยงานที่จะทำหน้าที่ Data Controller หรือเป็น Data Processor ที่จะเก็บและประมวลผลข้อมูลส่วนบุคคลของพลเมืองจากประเทศในกลุ่ม EU จึงยิ่งต้องคำนึงถึงการปฏิบัติให้สอดคล้องกับมาตรการ GDPR ด้วยความระมัดระวัง

ยังมีความกังวลจากหลายฝ่ายที่เริ่มตระหนักถึงความสำคัญของ GDPR โดยมองว่าถึงแม้ผู้ประกอบการไทยอาจไม่โดนดำเนินคดีทางกฎหมายจากการไม่ปฏิบัติตามหรือปฏิบัติขัดกับหลักการ GDPR แต่โดยที่ธรรมชาติของการติดต่อธุรกิจระหว่างประเทศต้องมีการแลกเปลี่ยนข้อมูลระหว่างกันอยู่แล้ว หากฝ่ายผู้ประกอบการทางยุโรปเห็นว่าบริษัทคู่ค้าของไทยไม่สามารถปฏิบัติตาม GDPR บริษัท EU ก็จะไม่สามารถแลกเปลี่ยนข้อมูลกับบริษัทในไทย ซึ่งก็จะส่งผลให้ไม่สามารถทำธุรกิจธุรกรรมกันได้ในที่สุด

นอกจากนี้ EU อาจใช้มาตรการแทรกแซงทางการค้าอื่นๆ ในลักษณะเช่นเดียวกับการให้ “ใบเหลือง” ประเทศไทยจากกรณีปัญหา Illegal, Unreported and Unregulated (IUU) Fishing เมื่อเดือนเมษายน 2558 โดยระบุว่าเป็นประเทศที่ไม่ให้ความร่วมมือในการต่อต้านการทำประมงที่ผิดกฎหมาย ซึ่ง EU ได้ใช้มาตรการคว่ำบาตรการนำเข้าอาหารทะเลจากประเทศที่เพิกเฉยต่อการแก้ไขปัญหา IUU fishing

---

คำถามที่กำลังรอคำตอบ

- GDPR เป็นที่รับรู้ของพลเมืองโดยเฉพาะผู้ประกอบการในประเทศไทยมากน้อยเพียงใด
- GDPR จะมีผลกระทบต่อธุรกิจไม่ว่าจะเป็นธุรกิจขนาดใหญ่และขนาดเล็กหรือเปล่า
- หน่วยงานของรัฐหน่วยใดควรเป็นผู้เผยแพร่ความรู้ความเข้าใจและให้คำแนะนำเกี่ยวกับการปฏิบัติตามหลักเกณฑ์นี้ - กระทรวงพาณิชย์ กระทรวงต่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หรือสำนักนายกรัฐมนตรี หรือควรเป็นหน้าที่ขององค์กรภาคเอกชน หอการค้า สภาอุตสาหกรรม หรือสมาคมธนาคาร
- พลเมืองไทย ทั้งผู้ประกอบการธุรกิจหรือผู้บริโภค จะได้รับผลกระทบหรือไม่อย่างไรจากมาตรการนี้
- หน่วยงานของรัฐที่เก็บและประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตาม GDPR หรือไม่

คำถามเหล่านี้ล้วนกำลังรอคำตอบ!

โดยเฉพาะคำถามสุดท้าย –
คนไทยรู้จักและเข้าใจ GDPR กันหรือยัง?

---
25 July 2019 HRC@bangkok