GDPR's Global Reach

เขียนโดย Arthur Piper
แปลโดย สุวรรณา เจนสวัสดิ์พงศ์, CIA

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) ไปไกลทั่วโลกแล้ว คุณรู้แล้วหรือยัง

ตอนนี้ผู้ตรวจสอบภายในทั่วโลกกำลังเริ่มศึกษาว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มีผลต่อองค์กรที่ตนทำงานอยู่อย่างไร และต้องมีการดำเนินการอะไรบ้างเพื่อให้เป็นไปตามกฎหมาย

GDPR's Global Reach

ถ้าบริษัทห้างร้านของอเมริกาเชื่อว่าทะเลแอตแลนติกอันกว้างใหญ่จะสามารถขวางกั้นไม่ให้พวกเขาต้องทำตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้ ภาพฝันนั้นได้จางหายไปแล้วเมื่อวันที่ 21 มกราคม 2019 ที่ผ่านมา ซึ่งเป็นวันที่หน่วยงานที่กำกับดูแลเกี่ยวกับเรื่องความเป็นส่วนบุคคลของฝรั่งเศส คือ คณะกรรมการคุ้มครองข้อมูลแห่งชาติของประเทศฝรั่งเศส (Commission Nationale de l'informatique et des Libertés (CNIL)) ได้เรียกค่าปรับจากกูเกิลจำนวนประมาณ 50 ล้านยูโร (57 ล้านเหรียญสหรัฐ) ในข้อหา "ไม่โปร่งใส ให้ข้อมูลไม่เพียงพอ และขาดการยินยอมที่ถูกต้องเกี่ยวกับการโฆษณาส่วนบุคคล"

NOYB–European Center for Digital Rights and La Quadrature du Net — เป็นการรวมตัวกันของกลุ่มนักกิจกรรมหัวรุนแรงที่ต่อต้านการใช้ข้อมูลส่วนบุคคลอย่างไม่ถูกต้องจำนวน 2 กลุ่ม (หมายเหตุผู้แปล: ได้แก่ ศูนย์คุ้มครองการใช้สิทธิทางดิจิทัลของสหภาพยุโรป และกลุ่มเรียกร้องการใช้อินเทอร์เน็ตอย่างมีขอบเขต โดยกลุ่มนี้เรียกตัวเองว่า NOYB (None of your business) หรือ ไม่ใช่กงการของคุณ) ได้ร้องเรียนกรณีเกี่ยวกับบริษัทกูเกิลทันทีที่กฎหมาย GDPR มีผลบังคับเมื่อวันที่ 25 พฤษภาคม 2018 โดยกลุ่ม NOYB อ้างว่าผู้ใช้งานไม่สามารถให้การอนุญาตที่เฉพาะเจาะจงแก่กูเกิลในการดำเนินการกับข้อมูลส่วนบุคคลของตนได้ เนื่องจากข้อตกลงและเงื่อนไขของกูเกิลคลุมเครือไม่ชัดเจนเกินไป

หน่วยงานกำกับดูแลเห็นด้วยกับข้อร้องเรียนว่ามีการทำผิดกฎหมาย และในที่สุด การพิจารณาคดีแรกซึ่งเป็นคดีใหญ่ภายใต้กฎหมายใหม่ก็จบลงโดย CNIL ตัดสินว่ากูเกิลได้ละเมิดข้อกำหนดในเรื่องความโปร่งใสเนื่องจากหากลูกค้าของกูเกิลต้องการทราบว่าข้อมูลของตนได้ถูกใช้งานในเรื่องใดและอย่างไรบ้าง โดยเฉพาะบริการของกูเกิลที่เกี่ยวกับการติดตามสถานที่ตั้งทางภูมิศาสตร์ (geo-tracking service) ผู้ใช้งานจะต้องเปิดเข้าไปในหน้าต่างๆ ของเว็บไซต์กูเกิลถึง 5-6 หน้า แม้กระนั้นก็ตาม ข้อมูลก็ยังไม่ชัดเจนหรือไม่ครอบคลุมเพียงพอ นอกจากนั้น CNIL ยังกล่าวอีกว่า เนื่องจากบริษัทใช้งานข้อมูลส่วนบุคคลในการให้บริการหลายอย่างต่อๆ กันไป แต่วิธีการที่กูเกิลทำตามที่กฎหมายกำหนดเพื่อขอใช้ข้อมูลในการให้บริการแต่ละอย่างนั้นไม่ชัดเจนเกินไป

หน่วยงานกำกับดูแลยังพบอีกด้วยว่า วิธีการขอความยินยอมของกูเกิลที่ส่งโฆษณาเฉพาะบุคคลไปยังลูกค้าเป้าหมายนั้นไม่ถูกต้อง เนื่องจากมีการร้องเรียนกันว่าผู้ใช้งานกูเกิลต้องเข้าไปที่เมนู "ทางเลือกอื่น" เพื่อแก้ไขเกี่ยวกับการอนุญาตให้ใช้งานข้อมูลของตัวเอง ซึ่งช่องที่ระบุว่ายินยอมได้ถูกระบบทำเครื่องหมายติ๊กไว้ให้ล่วงหน้า (pre-ticked) อยู่แล้ว และที่สำคัญ CNIL พบว่า ในการที่ผู้ใช้งานจะสร้างบัญชีของตนในระบบผู้ใช้งานจะต้องยินยอมให้บริษัททำการประมวลผลข้อมูลหลายๆ อย่าง อันได้แก่ การโฆษณาที่ส่งเฉพาะบุคคล การจดจำเสียงพูดและอื่นๆ ถูกรวมอยู่ในสัญญาฉบับเดียว ทั้งนี้ CNIL สรุปว่า "กฎหมาย GDPR จะถือว่าการให้การอนุญาตต้อง "เฉพาะเจาะจง" ให้ชัดเจนสำหรับแต่ละวัตถุประสงค์ของการใช้ข้อมูล"

GDPR's Global Reach

กฎหมาย GDPR เป็นแค่บทเริ่มต้น

ในขณะที่กูเกิลอุทธรณ์คดีต่อสภาแห่งรัฐของฝรั่งเศส (เป็นหน่วยงานรัฐบาลระดับชาติในฝรั่งเศส) CNIL ได้ให้เหตุผลที่ชี้ให้เห็นว่า หน่วยงานกำกับดูแลตีความการบังคับใช้กฎหมาย GDPR ในประเด็นที่สำคัญต่อองค์กรต่างๆ ทั่วโลกอย่างไร และจะถูกปรับอย่างไร ยิ่งไปกว่านั้นกฎหมาย GDPR มีแนวโน้มที่จะส่งผลให้องค์กรต่างๆ ทั่วโลกต้องปรับเปลี่ยนแนวทางการจัดการข้อมูลส่วนบุคคล ดังนั้น จึงไม่น่าแปลกใจว่าเมื่อวันที่กฎหมาย GDPR มีผลใช้บังคับ ผู้ตรวจสอบภายในที่รู้สึกว่าตนได้ก้าวข้ามเส้นชัยมาแล้วแต่กลับรู้สึกว่าจริงๆ แล้วการแข่งขันนั้นเพิ่งเริ่มต้น

แจน เฮิร์ทซเบิร์ก ที่ปรึกษาด้านการใช้ข้อมูลส่วนบุคคล และศาสตราจารย์ผู้ทรงคุณวุฒิแห่งมหาวิทยาลัย เดอ ปอล ที่ชิคาโก้ กล่าวว่า "มีองค์กรในสหรัฐหลายแห่งรู้สึกอยากให้องค์กรตนได้เริ่มปฏิบัติตามกฎหมาย GDPR มาตั้งแต่ก่อนหน้านี้แล้ว" และกล่าวเพิ่มเติมว่า เมื่อปีที่แล้วองค์กรต่างๆ เหล่านั้นเพิ่งจะแก้ไขนโยบายและประกาศเกี่ยวกับการใช้ข้อมูลส่วนบุคคลก่อนที่กฎหมาย GDPR จะมีผลบังคับใช้ไม่นาน องค์กรเหล่านั้นได้วางแผนที่จะประเมินความเสี่ยงทั่วทั้งองค์กรเกี่ยวกับกฎหมาย GDPR ให้ "เป็นระดับสูงสุด" ภายในปีถัดมา และให้มีการตรวจสอบการปฏิบัติตามข้อกำหนดในกฎหมาย GDPR ด้วย

ทั้งนี้ การเพิ่งให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลถือได้ว่าอยู่ในช่วงเวลาที่เหมาะสม เพราะหลักปรัชญาที่เป็นรากฐานของกฎหมาย GDPR คือ การหาหนทางในการสร้างหลักเกณฑ์สำหรับระเบียบใหม่ๆ ของประเทศต่างๆ ทั่วโลก กล่าวคือ ลูกค้าจะต้องเลือกได้อย่างชัดเจนว่าบริการที่ตนจะเข้าไปใช้คืออะไร การอนุญาตให้ข้อมูลของตนถูกใช้นำไปประมวลผลเพื่อใช้งานได้ต้องชัดแจ้ง ลูกค้าต้องมีสิทธิ์รู้ว่าองค์กรมีข้อมูลอะไรของตนบ้างและนำมันไปใช้เพื่อการใด และหากพบว่ามีการละเมิดอย่างร้ายแรงเกิดขึ้น องค์กร/บริษัทจะต้องมีกระบวนการที่ฉับไวในการแจ้งต่อทั้งหน่วยงานกำกับดูแลและลูกค้า ยกตัวอย่างเช่น ที่สหภาพยุโรป กฎหมาย GDPR ได้ถูกขยายความให้ครอบคลุมถึงการสื่อสารทางอิเล็กทรอนิกส์ตามระเบียบการให้ความคุ้มครองข้อมูลส่วนบุคคลอิเล็กทรอนิกส์ฉบับใหม่ ซึ่งคาดว่าจะมีผลบังคับได้ในช่วงปลายปีนี้ กฎระเบียบเหล่านี้จะควบคุมการส่งข้อความและอีเมล์ที่ไม่พึงประสงค์ ทำให้ผู้ใช้งานเว็บไซต์สามารถกำหนดการบันทึกข้อมูลการเข้าเว็บไซต์ (cookie) ในโปรแกรมเรียกดูเว็บไซต์ในเครื่องของตน (browser) เพื่อให้สามารถเข้าถึงเว็บไซต์นั้นในครั้งต่อไปได้อย่างรวดเร็ว และจะทำให้หลักเกณฑ์ด้านการรักษาข้อมูลความลับเพื่อบังคับใช้กับบริษัทที่ทำธุรกิจเกี่ยวกับอินเทอร์เน็ตมีความเข้มข้นมากขึ้น

ถ้าไปดูนอกสหภาพยุโรป ปีที่แล้วสาธารณรัฐประชาชนจีน ได้ออกกลุ่มหลักเกณฑ์เกี่ยวกับ ความมั่นคงปลอดภัยทางไซเบอร์ การปกป้องข้อมูล และการถ่ายโอนข้อมูลข้ามประเทศ ซึ่งมีลักษณะคล้ายกับที่มีอยู่ในกฎหมาย GDPR ส่วนทางด้านสหรัฐอเมริกา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคแห่งรัฐแคลิฟอร์เนีย 2018 (California Consumer Privacy Act of 2018) ที่จะมีผลบังคับในปี 2020 ก็มีข้อกำหนดให้มีทางเลือกที่จะขอไม่ใช้บริการ มีเรื่องกฎเกณฑ์เกี่ยวกับความโปร่งใส และสิทธิของผู้บริโภคที่จะถูกลืม (rights for customers to be forgotten: หมายเหตุ — สิทธิที่จะถูกลืม หมายถึง สิทธิของปัจเจกบุคคลที่จะร้องขอให้อีกฝ่าย ซึ่งจะเป็นปัจเจกบุคคลก็ดีหรือองค์กรก็ดี ที่มีข้อมูลส่วนบุคคลของเขาไว้ในครอบครองทำการลบข้อมูลส่วนบุคคลของตนออกเสีย เนื่องจากไม่ยินยอมจะให้มีการใช้ข้อมูลนั้นอีกต่อไป) ซึ่งคล้ายคลึงกับเนื้อหาที่มีอยู่ในกฎหมาย GDPR

GDPR's Global Reach

มีผู้ตรวจสอบภายในกำลังดำเนินการเพื่อให้ตนมีความเข้าใจมากขึ้น ในแนวทางที่หน่วยงานกำกับดูแลจะใช้ เพื่อให้คำแนะนำและบทลงโทษมีความสมดุลกัน และก็มีผู้ตรวจสอบภายในอีกส่วนหนึ่งที่กำลังยุ่งอยู่กับการสร้างเครือข่ายทั้งภายในและภายนอกองค์กร เพื่อช่วยพวกเขาให้มีความเข้าใจในหลักเกณฑ์และผลที่จะมีต่อองค์กรของตน อย่างไรก็ตาม ถึงแม้ว่าทุกคนดูจะต้องเพิ่มความเชี่ยวชาญของตนเองในด้านเทคโนโลยีสารสนเทศให้มากขึ้น แต่การทำความเข้าใจในประเด็นทางกลยุทธ์ก็ถือเป็นหัวใจสำคัญ

แนวทางของหน่วยงานกำกับดูแล

กฎหมาย GDPR มีผลบังคับกับสถานประกอบการทุกแห่งที่มีข้อมูลส่วนบุคคลของประชาชนในสหภาพยุโรป และรวมไปถึงธุรกิจที่ตั้งอยู่นอกภูมิภาคตามกฎที่สหภาพยุโรปกำหนดไว้ด้วย ในกรณีของกูเกิลที่เกิดขึ้นในปีนี้ CNIL แสดงให้เห็นอย่างชัดเจนว่า การพิจารณาข้อร้องเรียนที่เกิดขึ้นกับบริษัทในสหรัฐอเมริกาและบริษัทอื่นที่ตั้งอยู่นอกสหภาพยุโรปไม่ได้แตกต่างไปจากกรณีที่เกิดขึ้นในยุโรป ถึงแม้ว่าสำนักงานใหญ่ประจำภาคพื้นยุโรปของกูเกิลจะตั้งอยู่ที่กรุงดับลิน ประเทศไอร์แลนด์ CNIL ก็แจ้งข้อหาต่อบริษัท กูเกิล จำกัด (มหาชน) ที่สหรัฐอเมริกา เนื่องจากสำนักงานกูเกิลที่สหรัฐอเมริกาเป็นผู้มีอำนาจตัดสินว่าข้อมูลส่วนบุคคลที่แอปพลิเคชันแอนดรอยด์ของตนรวบรวมและจัดเก็บไว้นั้นจะถูกนำมาใช้งานอย่างไร และบริษัทกูเกิลที่สหรัฐอเมริกาซึ่งเป็นบริษัทแม่ ต้องมีความรับผิดชอบทางกฎหมายต่อการปฏิบัติตามกฎหมาย GDPR ดังนั้น CNIL จึงคำนวณค่าปรับจากรายได้รวมของบริษัทแม่ ซึ่งในปี 2017 มีจำนวน 110,000 ล้านเหรียญสหรัฐ ค่าปรับจึงเป็น 4,400 ล้านเหรียญสหรัฐ ไม่ใช่แค่ 57 ล้านเหรียญสหรัฐ

สำนักงานคณะกรรมการด้านข้อมูลข่าวสาร (Information Commissioner's Office — ICO) ซึ่งเป็นหน่วยงานกำกับดูแลของสหราชอาณาจักรกล่าวว่า ค่าปรับไม่ได้แสดงให้เห็นถึงภัยสูงสุดที่เกิดจากกฎหมาย GDPR ที่สามารถเกิดขึ้นได้กับบริษัทจริงๆ แล้วแนวคิดในการกำหนดให้ค่าปรับมีจำนวนสูงมากๆ เป็น "ตำนานเรื่องที่ 1"

ในการทำให้เป็นที่เข้าใจกันว่าหน่วยงานกำกับดูแลตีความและใช้อำนาจใหม่นี้อย่างไร โดย เดโบรา บิอาซูติ หัวหน้าคณะเจ้าหน้าที่ด้านการสื่อสารของ ICO กล่าวว่า "ICO ตั้งใจที่จะใช้อำนาจและการแทรกแซงเป็นเครื่องมือในการให้ความรู้และสนับสนุนองค์กรต่างๆ ให้ปฏิบัติตามภาระหน้าที่ในการคุ้มครองข้อมูลให้ปลอดภัย ส่วนการเรียกค่าปรับตามที่เคยเป็นมา และที่จะเป็นเช่นนั้นต่อไป จะเป็นทางเลือกสุดท้าย"

ในขณะที่มีการเผยแพร่บทความนี้ (มีนาคม 2019) สหราชอาณาจักรอาจออกจากการเป็นสมาชิกสหภาพยุโรปไปแล้ว โดยไม่มีข้อตกลงที่เป็นทางการเกี่ยวกับการกำกับดูแลการใช้ข้อมูลของประชาชนระหว่างสหราชอาณาจักรและสหภาพยุโรป ซึ่งถ้าเป็นเช่นนั้นจริง พรบ. คุ้มครองข้อมูล 2018 (2018 Data Protection Act) ที่เป็นเกือบเสมือนกฎหมาย GDPR ฉบับร่างจะถือเป็นกฎหมายของสหราชอาณาจักรด้วย

หน่วยงานกำกับดูแลทั้งหลายกำลังร่วมมือกับกิจการต่างๆ เพื่อช่วยกิจการเหล่านั้นให้ปฏิบัติให้ถูกต้องตามกฎหมาย แต่ก็พร้อมที่จะเรียกค่าปรับ "ตามสัดส่วน" ทุกครั้งที่ทราบถึงการไม่ถือปฏิบัติตามกฎหมาย

ico.
Information Commissioner's Office

GDPR's Global Reach

ข้อบ่งชี้แรกๆ คือ หน่วยงานกำกับดูแลทั้งหลายกำลังร่วมมือกับกิจการต่างๆ เพื่อช่วยกิจการเหล่านั้นให้ปฏิบัติให้ถูกต้องตามกฎหมาย แต่ก็พร้อมที่จะเรียกค่าปรับ "ตามสัดส่วน" ทุกครั้งที่ทราบถึงการไม่ถือปฏิบัติตามกฎหมาย ซึ่งสามารถเห็นได้จากกรณีต่างๆ ที่เกิดขึ้นก่อนกรณีกูเกิล โดยกรณีต่างๆ เหล่านั้นเป็นกิจการที่มีขนาดเล็กกว่ากูเกิลมาก

ยกตัวอย่างเช่น ในเดือนธันวาคม 2018 CNIL ได้ปิดคดีการขออนุญาตการใช้ข้อมูลตามกฎหมาย GDPR โดยบริษัทที่เกิดเหตุเป็นบริษัทโฆษณาทางเทคโนโลยีขนาดเล็กของฝรั่งเศสชื่อฟิดซ์อัพ (Fidzup) จากข้อมูลในวารสารออนไลน์ที่ชื่อเทคครันช์ บริษัทฟิดซ์อัพได้ร่วมกันกับ CNIL สร้างแบบฟอร์มยินยอมที่มีรายละเอียดมากขึ้น เพื่อให้ลูกค้าแต่ละคนเลือกว่าจะใช้หรือไม่ใช้บริการใดของบริษัทบ้าง โดยแยกเป็นรายบริการซึ่งสิ่งที่ CNIL ดำเนินการนี้สะท้อนให้เห็นได้ถึงแนวทางที่ CNIL ใช้ในการพิจารณากรณีกูเกิล

> **"เนื่องจากเรื่องนี้มีความชัดเจนว่าเป็นปรากฏการณ์ระดับโลก หน่วยงานกำกับดูแลในภูมิภาคยุโรปจึงควรดำเนินการโดยคำนึงถึงผู้ที่อยู่นอกภูมิภาคแต่ต้องปฏิบัติตามกฎหมายให้มากกว่าที่เป็นอยู่ด้วย"**
>
> แจน เฮิร์ทซเบิร์ก

โอลิเวอร์แมกนัน-เซาริน ประธานเจ้าหน้าที่บริหารของบริษัทฟิดซ์อัพ ได้บอกกับ*วารสารเทคครันช์*ว่า "ขณะนี้ เรามีอะไรบางอย่างที่อยู่ระหว่างการขอแนวทางจาก CNIL ตั้งแต่แรก ซึ่งเป็นเหมือนหนังสือเล่มโต กับการเก็บรวบรวมใบให้ความยินยอมซึ่งสั้นมากและข้อมูลก็ไม่ถูกต้อง ก่อนที่ CNIL จะออกคำเตือนแล้ว" เขาได้ยอมรับว่า ยังต้องมีการแก้ไขแบบฟอร์มคำยินยอมอีกมาก นอกจากนั้น บริษัทยังต้องมีการเปลี่ยนวิธีการทำงานของเทคโนโลยีต่างๆ ด้วย ตัวอย่างเช่น ถ้าลูกค้าเลือกขอไม่ให้ส่งพิกัดของตนไปให้บริษัทโฆษณา คำสั่งให้ตรวจจับพิกัดของลูกค้าในโปรแกรมก็จะต้องยังคงทำงานอยู่ แต่ไม่ส่งข้อมูลออกไปให้บริษัทโฆษณา

ค่อย ๆ เป็น ค่อย ๆ ไป

การวิจัยของสมาคมผู้ตรวจสอบภายใน (IIA) เมื่อเร็วๆ นี้ แสดงผลว่า ยังไม่เป็นที่แน่ชัดว่า ผู้ตรวจสอบภายในสามารถจับประเด็นของกฎหมาย GDPR (ซึ่งเป็นกฎหมายนอกเขตดินแดนของตน) ได้มากน้อยเพียงใด การวิจัยประจำปี 2019 ของ IIA ประจำภาคพื้นอเมริกาเหนือ (The 2019 North American Pulse of Internal Audit) พบว่า ถึงแม้จะมีหัวหน้าหน่วยงานตรวจสอบภายในมากถึง 70% แสดงความกังวลอย่างมากว่าเรื่องที่เกี่ยวกับข้อมูลส่วนบุคคลอาจทำให้ชื่อเสียงของบริษัทเสียหายอย่างร้ายแรง แต่มีเพียง 29% ที่แสดงความกังวลอย่างมากต่อการปฏิบัติตามกฎหมาย GDPR และมีจำนวนเพิ่มขึ้นเป็น 62% หากนับเฉพาะกลุ่มหัวหน้าที่มาจากบริษัทขนาดใหญ่โดยในรายงานผลการวิจัยระบุว่า "ผลการวิจัยแสดงให้เห็นว่าอาจมีความเข้าใจที่ไม่ถูกต้องเกี่ยวกับการบังคับใช้ หลักเกณฑ์การป้องกันความปลอดภัยของข้อมูล และกฎการคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่" และในรายงานดังกล่าวได้แสดงความเห็นเพิ่มเติมเกี่ยวกับความเข้าใจที่ไม่ถูกต้องนั้นว่าอาจมีหัวหน้าหน่วยงานตรวจสอบภายในบางส่วนเชื่อว่า ธุรกิจที่ตนทำงานอยู่นั้นไม่อยู่ในความครอบคลุมของกฎหมายในขณะที่ข้อเท็จจริงของหลักเกณฑ์ไม่ได้พิจารณาตามที่ตั้งของบริษัทผู้ให้บริการ แต่พิจารณาตามที่อยู่ของผู้ใช้บริการซึ่งข้อมูลของเขาถูกเก็บรวบรวมมา

เฮิร์ทซเบิร์ก กล่าวว่า การที่บริษัทตอบสนองต่อการปฏิบัติตามกฎหมาย GDPR อย่างล่าช้านั้น ส่วนหนึ่งอาจเนื่องมาจากการขาดความรู้เกี่ยวกับข้อกำหนดของกฎหมาย และขาดความชัดเจนว่าจะปฏิบัติตามกฎหมายอย่างไร โดยเฉพาะการที่สหภาพยุโรปขาดความใส่ใจในการให้ความรู้ต่อธุรกิจนอกภูมิภาคยุโรป

GDPR's Global Reach

คือ "เนื่องจากเรื่องนี้มีความชัดเจนว่าเป็นปรากฏการณ์ระดับโลก หน่วยงานกำกับดูแลในภูมิภาคยุโรปจึงควรดำเนินการโดยคำนึงถึงผู้ที่อยู่นอกภูมิภาคแต่ต้องปฏิบัติตามกฎหมายให้มากกว่าที่เป็นอยู่ด้วย"

เฮิร์ทซเบิร์ก เพิ่มเติมว่า "การขาดความตระหนักในข้อกำหนดของกฎหมาย GDPR เป็นประเด็นที่น่าวิตกทั้งต่อคณะกรรมการ ผู้บริหารและบุคลากรของบริษัท" โดยปกติผู้ตรวจสอบภายใน และผู้ที่อยู่ในวิชาชีพกำกับดูแลการถือปฏิบัติตามกฎหมาย มักจะพบความยากลำบากในการทำให้ผู้มีส่วนได้เสียให้ความสนใจในประเด็นที่ดูจะเป็นเรื่องของแค่ประเทศแถบยุโรป และ "ขณะนี้กระแสความสดใหม่ของกฎหมาย GDPR เริ่มซาลงด้วย จึงมีข้อกังวลเกิดขึ้นว่า ต่อไปข้อบังคับนี้ก็คงจะค่อยๆ ได้รับความสนใจน้อยลงๆ"

นอกจากนั้น เฮิร์ทซเบิร์ก ระบุว่า ในเชิงการบริหารหน่วยงานตรวจสอบภายใน หัวหน้าหน่วยงานตรวจสอบภายในและผู้อำนวยการตรวจสอบภายใน อาจไม่มั่นใจที่จะจ้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ และด้านการคุ้มครองข้อมูลส่วนบุคคลเข้ามาร่วมทีม แต่กลับเลือกที่จะไปขอคำปรึกษาจากที่ปรึกษาทั่วไป หัวหน้าคณะเจ้าหน้าที่ด้านความปลอดภัยของข้อมูลสารสนเทศรวมทั้งหัวหน้าคณะเจ้าหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ช่วยจับประเด็นสำคัญของกฎหมายและตีความถึงสิ่งที่ต้องดำเนินการ และยังมีการไปขอความช่วยเหลือจากที่ปรึกษาที่เป็นบุคคลที่สามอีกด้วย

ในภาพรวม หัวหน้าหน่วยงานตรวจสอบภายในต้องสร้างให้เกิดความตระหนักเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ที่มีหน้าที่รับผิดชอบในการปฏิบัติงานของบริษัทมีความเข้าใจอย่างชัดเจนว่าตนคือ "เจ้าของ" ข้อมูลซึ่งตนได้เก็บรวบรวมและนำไปใช้งาน ซึ่งในการดำเนินการเช่นนั้นจะทำให้ผู้ปฏิบัติงานมีความเข้าใจในความจำเป็นที่ต้องมีและประเด็นปัญหาต่างๆ ในการรวบรวม และปกป้องข้อมูลส่วนบุคคล และเฮิร์ทซเบิร์กยังกล่าวถึงสิ่งที่เป็นปัญหามากด้วยว่า ธุรกิจยังมีความเข้าใจที่ไม่ชัดเจนว่า ในที่สุดแล้ว คนไหน (ต้องระบุชื่อ) ที่จะต้องมีความรับผิดชอบต่อข้อมูลของส่วนบุคคลที่องค์กรเป็นเจ้าของอยู่

เฮิร์ทซเบิร์ก กล่าวว่า "ข้อกำหนดเกี่ยวกับการปฏิบัติตามกฎหมาย กฎระเบียบทั้งหลาย ก็เหมือนกับกฎหมาย GDPR ที่จะบังคับให้เกิดการเปลี่ยนแปลงในการจัดการข้อมูลที่บริษัทมีอยู่" และ "สำหรับหัวหน้าหน่วยงานตรวจสอบภายในแล้ว มันไม่ใช่แค่เรื่องการคุ้มครองข้อมูลส่วนบุคคล แต่มันมีเรื่องความถูกต้อง เชื่อถือได้ของข้อมูลทั่วทั้งองค์กรด้วย มันจึงหมายความว่า ผู้ตรวจสอบภายในทั้งหลายต้องให้ความสำคัญต่อข้อมูลมากกว่าที่ที่เคยเป็นมา และในการให้ความเชื่อมั่น ผู้ตรวจสอบภายในจะต้องปรับแนวทางการปฏิบัติงานโดยเพิ่มความใส่ใจในการลงรายละเอียดเกี่ยวกับข้อมูลให้มากขึ้นด้วย"

> **"ดังนั้น ผู้ตรวจสอบภายในจึงจำเป็นต้องช่วยธุรกิจให้เข้าใจให้ได้ว่า ข้อมูลคือสินทรัพย์ที่มีความสำคัญมาก และธุรกิจได้คุ้มครองให้มันมีความปลอดภัยได้ รวมทั้งใช้มันในการทำให้ธุรกิจเจริญเติบโตอย่างก้าวกระโดดได้อย่างที่ควรจะเป็นแล้วหรือยัง"**
>
> ดอร์มินิค วินเซ็นติ

GDPR's Global Reach

ประเด็นทางธุรกิจ

ดอร์มินิค วินเซ็นติ หัวหน้าหน่วยงานตรวจสอบภายในของบริษัท อูเบอร์ และอดีตรองกรรมการผู้อำนวยการด้านการตรวจสอบภายในของบริษัท นอร์ดสตรอม ที่ตั้งอยู่ที่เมืองซีแอตเทิล กล่าวว่า ในตอนแรกประเมินกันว่าความเสี่ยงจากเรื่องนี้ที่มีต่อธุรกิจห้างสรรพสินค้าน่าจะต่ำกว่าธุรกิจค้าปลีกขนาดใหญ่ทางออนไลน์ แต่ปรากฏว่าการประเมินนั้นไม่ถูกต้อง เนื่องจากคนในภูมิภาคยุโรปไม่ค่อยซื้อของออนไลน์ ดังนั้น "เราจึงใช้โอกาสนี้ในการกระตุ้นให้ฝ่ายบริหารเตรียมการเกี่ยวกับเรื่องนี้เนื่องจากเรารู้สึกว่ามันจะไม่ได้มีแค่กฎหมาย GDPR ที่ต้องมีการถือปฏิบัติ แต่มันน่าจะมีอย่างอื่นที่คล้ายๆ กับ GDPR ที่บริษัทต้องเตรียมดำเนินการเพิ่มเติมด้วย"

และก็เป็นเช่นนั้นจริง เพราะหลังจากที่กฎหมาย GDPR มีผลบังคับ รัฐแคลิฟอร์เนียก็ได้ออกกฎหมายคุ้มครองผู้บริโภค วินเซ็นติจึงกล่าวต่อไปว่า เธอไม่แปลกใจเลย หากสหรัฐจะมีกฎหมายทำนองเดียวกันออกมาอีกเป็นชุด และอธิบายต่อว่า "นั่นเป็นเพราะรัฐแคลิฟอร์เนียมีความสำคัญต่อธุรกิจของสหรัฐนั่นเอง" และ "ถ้าคุณกำลังจะต้องถือปฏิบัติตามกฎหมาย GDPR คุณไม่ใช่แค่ต้องปรับระบบเพียงให้แค่รองรับลูกค้าที่อยู่ในรัฐแคลิฟอร์เนียเนื่องจากมันจะเป็นการยากเกินไปที่จะแบ่งแยกลูกค้าของคุณ แต่คุณควรปรับวิธีการดำเนินการให้รองรับกฎระเบียบที่มีผลกระทบกับฐานลูกค้ากลุ่มที่ใหญ่ที่สุดของคุณไปเลย"

วินเซ็นติ กล่าวว่า ในการทำความเข้าใจกับความสำคัญของกฎ ระเบียบต่างๆ เธอคาดว่าผู้ตรวจสอบภายในส่วนใหญ่จะก้าวไปล่วงหน้าก่อนที่การเปลี่ยนแปลงจะเกิดขึ้นแล้ว ซึ่งโดยปกติในขั้นแรก ผู้ตรวจสอบภายในมักจะเข้าใจไว้ก่อนว่าองค์กรมีระบบการกำกับดูแลข้อมูลที่ไม่เพียงพอ ดังนั้น การที่บริษัทจะต้องปฏิบัติตามกฎหมาย GDPR จึงเป็นโอกาสอันดีที่ผู้ตรวจสอบจะเริ่มด้วยการพูดถึงวิธีการที่ธุรกิจควรบริหารและควบคุมข้อมูลให้มีประสิทธิผลได้ ขั้นที่ 2 เนื่องจากจุดอ่อนของการกำกับดูแลข้อมูลทำให้การปฏิบัติตาม GDPR กลายเป็นประเด็นทางธุรกิจแทนที่จะเป็นเพียงประเด็นทางเทคโนโลยีสารสนเทศ

"ดังนั้น ผู้ตรวจสอบภายในจึงจำเป็นต้องช่วยธุรกิจให้เข้าใจให้ได้ว่า ข้อมูลคือสินทรัพย์ที่มีความสำคัญมาก และธุรกิจได้คุ้มครองให้มันมีความปลอดภัยได้ รวมทั้งใช้มันในการทำให้ธุรกิจเจริญเติบโตอย่างก้าวกระโดดได้อย่างที่ควรจะเป็นแล้วหรือยัง"

> "ถ้างานตรวจสอบภายในได้รับการยอมรับโดยมีที่นั่งในที่ประชุมของทั้งฝ่ายบริหารและคณะกรรมการตรวจสอบ ผู้ตรวจสอบจะสามารถประเมินได้ว่าฝ่ายบริหารได้เฝ้าระวังการเปลี่ยนแปลงของสภาพแวดล้อมในการดำเนินธุรกิจมากน้อยเพียงใด"
>
> เจมส์ ไรน์ฮาร์ด

ต้นแบบ และกลยุทธ์

เจมส์ ไรน์ฮาร์ด ผู้อำนวยการสำนักตรวจสอบภายในของกลุ่มบริษัทที่ดินไซมอน ที่เมืองกรีนวูด รัฐอินเดียนา กล่าวว่า เนื่องจากกฎหมายแบบ GDPR มีผลกระทบกว้าง ธุรกิจจึงอาจต้องวางแผนกลยุทธ์ของตนอีกครั้ง ยกตัวอย่างเช่น เนื่องจากอาจมีบางประเทศไม่อนุญาตให้มีการถ่ายโอนข้อมูลข้ามพรมแดน ดังนั้น แทนที่บริษัทจะออกแบบหรือคิดวิธีการให้มีการใช้ช่องทางที่เป็นแบบออนไลน์โดยข้อมูลจะถูกจัดเก็บไว้ในเซิร์ฟเวอร์กลาง

GDPR's Global Reach

บริษัทอาจจำเป็นต้องกระจายข้อมูลที่จัดเก็บมาไว้ในหลายประเทศ เนื่องจากบางประเทศอาจจะห้ามการโอนย้ายข้อมูลข้ามแดน ซึ่งวิธีเช่นนี้อาจต้องแลกมาด้วยค่าใช้จ่าย การเข้าถึงข้อมูล และความอยู่รอดของวิธีนี้

ไรน์ฮาร์ดกล่าวต่อไปว่า "ถ้างานตรวจสอบภายในได้รับการยอมรับโดยมีที่นั่งในที่ประชุมของทั้งฝ่ายบริหารและคณะกรรมการตรวจสอบ ผู้ตรวจสอบจะสามารถประเมินได้ว่าฝ่ายบริหารได้เฝ้าระวังการเปลี่ยนแปลงของสภาพแวดล้อมในการดำเนินธุรกิจมากน้อยเพียงใด" และ "ถ้าไม่ได้เข้าไปร่วมกับฝ่ายบริหารเช่นนั้นแล้ว ปัญหาสำหรับผู้ตรวจสอบก็จะเริ่มมากขึ้น"

ไรน์ฮาร์ดกล่าวว่า หัวหน้าหน่วยงานตรวจสอบภายในอาจต้องเสริมขีดความสามารถด้านเทคโนโลยีสารสนเทศให้คณะผู้ตรวจสอบภายในเพื่อให้สามารถสอบทานเกี่ยวกับข้อมูลส่วนบุคคลที่ซับซ้อนได้ สามารถติดตามวิธีการรักษาความปลอดภัยให้แก่ข้อมูลเมื่อข้อมูลนั้นถูกส่งผ่านไปตามขั้นตอนการให้บริการที่มีความเป็นดิจิทัลเพิ่มขึ้นมากทุกขณะได้

และไรน์ฮาร์ดกล่าวเพิ่มเติมว่า "ผู้ตรวจสอบภายในจำเป็นต้องพึ่งพาที่ปรึกษาด้านกฎหมายให้ช่วยตีความว่าข้อมูลแต่ละอย่างจะถูกนำไปใช้ประโยชน์อะไร และต้องทำอย่างไรจึงจะเรียกได้ว่าให้ความปลอดภัยแก่ข้อมูลนั้นแล้ว" และว่า "โดยปกติ หากบริษัทตีความทางกฎหมายไม่ถูกต้อง ความเห็นของผู้ตรวจสอบภายในจากการทดสอบหรือพิสูจน์การปฏิบัติตามกฎหมายก็จะไม่ถูกต้องด้วย" ดังนั้น การเพิ่มขีดความสามารถทางวิชาชีพของผู้ตรวจสอบภายในจะทำให้ผู้ตรวจสอบสามารถเปรียบเทียบการปฏิบัติของบริษัทที่ตนทำงานกับบริษัทอื่นที่เป็นคู่เทียบ และสามารถค้นหาแนวความคิดกลับมาเป็นข้อมูลให้กับบริษัทที่ตนทำงานได้

ค้นหาความหมาย

เจมส์ คาสโตร-เอ็ดเวิร์ดส ซึ่งเป็นหุ้นส่วนของบริษัทให้คำปรึกษาด้านกฎหมายเวดเลค เบล ที่ตั้งอยู่ที่ลอนดอน กล่าวว่า ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน บริษัทก็ต้องพยายามหาทางทำความเข้าใจให้ได้ว่ากฎหมาย GDPR มีความหมายในทางปฏิบัติอย่างไรและได้เล่าว่า "เราได้ยินมาว่ามีบริษัทหลายๆ บริษัทที่ทำเอกสารเป็นร้อยๆ หน้าเพื่อขออนุญาตการเข้าถึงข้อมูล แต่นั่นไม่ใช่สิ่งที่กฎหมายกำหนดให้ทำ" และก็มีการพบเรื่องที่เกิดในทำนองเดียวกันนี้มากขึ้น คือ การทำในสิ่งที่กฎหมายไม่ได้กำหนด เช่น การรายงานการละเมิดข้อมูลโดยรายงานที่เป็นกรณีเล็กน้อย ข้อมูลที่ได้รับผลกระทบมีความเสี่ยงต่ำ (ได้แก่ชื่อและที่อยู่ของประชาชน) หรือที่ได้ทำการเข้ารหัสข้อมูลและรักษาความปลอดภัยให้ข้อมูลไว้อย่างเหมาะสมแล้ว

คาสโตร-เอ็ดเวิร์ดสเพิ่มเติมว่า "ผู้ตรวจสอบภายในกำลังต้องการสนใจมากขึ้นมากกับการปฏิบัติตามหลักเกณฑ์การปกป้องข้อมูล" การดำเนินการอาจรวมไปถึงการให้ความเชื่อมั่นเกี่ยวกับความเข้าใจของบริษัทในเรื่องที่เป็นสาระสำคัญเพื่อให้ฝ่ายบริหารไม่ต้องเสียเวลาไปกับการรายงานที่มากเกินไป ตั้งแต่กฎหมาย GDPR มีผลบังคับใช้ สำนักงาน ICO ได้แสดงความเห็นในวงกว้างเกี่ยวกับการรายงานการละเมิดข้อมูลส่วนบุคคลที่มากจนเกินไป หลายกรณีถูกรายงานในลักษณะการเตือน ในขณะที่การปฏิบัติในข้อที่จำเป็น ซึ่งคือการบันทึกเหตุการณ์ที่เกิดขึ้น รวมทั้งคำอธิบายเมื่อตัดสินใจที่จะไม่รายงาน ซึ่งอาจถูกมองข้ามไป

คาสโตร-เอ็ดเวิร์ดสกล่าวว่า การบังคับใช้กฎหมายจะค่อยๆ ช่วยให้ธุรกิจเข้าใจกฎหมาย GDPR มากขึ้น แต่ความเสี่ยงด้านกฎหมายที่เกิดขึ้นใหม่จะยังคงเกิดขึ้นต่อไป

> "ผู้ตรวจสอบภายในกำลังต้องการสนใจมากขึ้นมากกับการปฏิบัติตามหลักเกณฑ์การปกป้องข้อมูล"
>
> เจมส์ คาสโตร-เอ็ดเวิร์ดส

GDPR's Global Reach

ปีที่แล้ว ซูเปอร์มาร์เก็ตที่สหราชอาณาจักรที่ชื่อ มอริสัน พบว่าตัวเองถูกฟ้องร้องโดยตัวแทนของกลุ่มบุคคลซึ่งที่ในสหรัฐอเมริกาเรียกการฟ้องร้องเช่นนี้ว่า คลาส แอคชั่น โดยผู้ฟ้องร้องนั้นเป็นตัวแทนของพนักงานกว่า 5,500 คน จากบุคลากรประมาณ 100,000 คนของมอริสัน ซึ่งข้อมูลส่วนตัวของพวกเขาถูกอดีตพนักงานที่ไม่พอใจในมอริสันปล่อยออกไปทางอินเทอร์เน็ต คดีนี้ถือได้ว่าเป็นคดีแรกก่อนที่จะมีคดีอื่นเกิดขึ้นในทำนองเดียวกันอีกหลายคดี โดยมีทนายความคนหนึ่งของสหราชอาณาจักรเป็นผู้ดำเนินการให้โดยอ้างอิงหลักกฎหมายจารีตประเพณีที่ได้มีการปรับปรุงล่าสุดเมื่อเร็วๆ นี้ ซึ่งการปรับปรุงนั้นก็คือการกำหนดหลักการว่าหากบุคคลใดได้รับผลกระทบจากการที่ข้อมูลส่วนบุคคลของตนถูกละเมิด ให้สามารถเรียกร้องค่าชดเชยความเสียหายได้

คาสโตร-เอ็ดเวิร์ดสกล่าวเพิ่มเติมอีกว่า "เรื่องนี้ยังเป็นช่วงเริ่มต้น แต่ยังสามารถกลายเป็นความเสี่ยงต่อธุรกิจที่ยิ่งใหญ่เทียบเท่าได้กับกิจกรรมการบังคับใช้กฎหมายของ ICO เนื่องจากจำนวนคนที่ได้รับผลกระทบจากการที่ข้อมูลของตนถูกละเมิดอย่างร้ายแรงมีเพิ่มขึ้น" และว่า "ผู้ที่ได้รับผลกระทบแต่ละคนนั้นต้องการค่าชดเชยเพียงจำนวนไม่มากไปจนถึงจำนวนที่สูงมากเพื่อนำไปแก้ไขความเสียหายก็ได้"

เรื่องนี้ตีความได้ว่า บริษัทในสหรัฐอเมริกาที่มีข้อมูลลูกค้าที่อยู่ในสหราชอาณาจักรอาจถูกฟ้องร้องโดยตัวแทนของกลุ่มบุคคล โดยคาสโตร-เอ็ดเวิร์ดส กล่าวว่า "ข้อเท็จจริงของเรื่องนี้คือ ICO และหน่วยงานกำกับดูแลอื่นมีทรัพยากรที่จำกัด แต่หากทนายความมีแรงและเวลาพอก็อาจยื่นฟ้องได้โดยเป็นตัวแทนให้แก่กลุ่มบุคคลจำนวนมากได้"

และบางทีบทเรียนสำคัญเรื่องกฎหมาย GDPR ที่จะมีต่อผู้ตรวจสอบภายใน ก็คือ กฎ ระเบียบใหม่นั้นไม่เพียงแต่จะเปลี่ยนกฎเรื่องข้อมูลส่วนบุคคลและการดำเนินการกับข้อมูลนั้น แต่มันเปลี่ยนเกมส์ด้วย ซึ่งผู้ที่จะชนะในเกมส์นั้นก็คือ ผู้ที่กำกับดูแลข้อมูลเป็นอย่างดี และให้ความสำคัญในการติดตามพัฒนาการของกฎระเบียบในทั่วโลกอย่างใกล้ชิด ทั้งนี้ ผู้ตรวจสอบภายในที่มีเครือข่ายที่เข้มแข็งทั้งในธุรกิจและนอกธุรกิจที่ตนทำงาน จะสามารถให้ข้อมูลสนับสนุนแก่คณะกรรมการบริษัทว่า GDPR จะส่งผลกระทบต่อการดำเนินงานและกลยุทธ์ของบริษัทได้อย่างไร ซึ่งผู้ตรวจสอบภายในที่สามารถทำเช่นนั้นได้ พูดง่ายๆ ก็คือคนสำคัญของบริษัทนั่นเอง

Arthur Piper เป็นนักเขียนที่มีความเชี่ยวชาญด้านการกำกับดูแล การตรวจสอบภายใน การบริหารความเสี่ยง และเทคโนโลยีสารสนเทศ