ผู้ตรวจสอบภายในสามารถช่วยนำทางให้องค์กรก้าวข้ามผ่านความเสี่ยงด้านการปฏิบัติตามกฎระเบียบที่เกิดขึ้นจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) ของสหภาพยุโรป

ขณะนี้ได้ผ่านพ้นวันที่ 25 พฤษภาคม ซึ่งต้องเริ่มปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) ของสหภาพยุโรป (EU) มาแล้ว ดังนั้น ผู้บริหารด้านการปฏิบัติตามกฎระเบียบน่าจะกำลังหายใจได้โล่งขึ้น แม้ว่าการปฏิบัติตามกฎหมายอย่างจริงจังเพิ่งจะเริ่มต้นขึ้น

GDPR ได้รวมกฎหมาย EU ฉบับต่างๆ ที่ปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคลไว้ด้วยกัน และได้ปรับเปลี่ยนทิศทางที่องค์กรใช้จัดการความเป็นส่วนตัวของข้อมูลเสียใหม่ GDPD ได้ขยายสิทธิส่วนบุคคลของพลเมืองและผู้มีถิ่นพำนักใน EU ให้กว้างขึ้นอย่างมาก และยังมีผลใช้บังคับกับองค์กรที่มีธุรกรรมกับบุคคลเหล่านั้น ไม่ว่าจะตั้งอยู่ ณ ที่แห่งใดก็ตาม องค์กรที่ไม่ปฏิบัติตาม GDPR มีโทษปรับสูงสุดถึง 20 ล้านยูโร หรือ 4% ของรายได้รวมทั่วโลกต่อปี แล้วแต่จำนวนใดจะสูงกว่า

การปฏิบัติตาม GDPR ต้องอาศัยความสนใจและความพยายามอย่างต่อเนื่อง ผู้ตรวจสอบภายในสามารถช่วยให้องค์กรลดความเสี่ยงจากการปฏิบัติตาม GDPR ได้ โดยการกำหนดวิธีการที่จะปรับปรุงการควบคุม การสร้างความตระหนักถึงความเสี่ยง และการให้ความเชื่อมั่นต่อการปฏิบัติตาม GDPR

การปรับปรุงการควบคุม

ผู้ตรวจสอบภายในสามารถช่วยองค์กรให้ก้าวผ่านจากช่วงเตรียมการไปสู่ช่วงของการนำ GDPR ไปปฏิบัติได้ กฎหมายฉบับนี้กำหนดให้องค์กรต้องให้ความสำคัญกับหัวข้อที่มุ่งเน้นด้านการควบคุมดังนี้

- ✓ ความถูกต้องแม่นยำ และคุณภาพ องค์กรต้องทำให้มั่นใจได้ว่าข้อมูลมีความถูกต้องแม่นยำ และเป็นปัจจุบัน และแต่ละบุคคลสามารถแก้ไขข้อมูลของตัวเองได้
- ✓ ความมั่นคงปลอดภัย และความเป็นส่วนตัวที่ออกแบบมา องค์กรต้องบันทึกข้อมูลการตัดสินใจที่จะแจ้งประชากร EU ว่า ข้อมูลของพวกเขาจะถูกใช้งานหรือมีข้อจำกัดอย่างไร และองค์กรต้องมีมาตรการควบคุมทั้งทางเทคนิค ทางการบริหาร และด้านความมั่นคงปลอดภัยทางกายภาพ/ความเป็นส่วนตัว เพื่อลดความเสี่ยงจากอันตรายที่อาจมีต่อข้อมูล
- ✓ การปกป้องความมั่นคงปลอดภัย บริษัทต้องทำให้มั่นใจได้ว่ามาตรการทางเทคนิค และทางด้านองค์กรได้ถูกดำเนินการเพื่อความเป็นส่วนตัวและความมั่นคงปลอดภัย

ผู้ตรวจสอบภายในควรทำงานกับฝ่ายบริหาร เพื่อกำหนดการควบคุมที่เกี่ยวข้องกับการนำเข้าข้อมูล ประเมินความถูกต้องแม่นยำของสารสนเทศ และเสนอแนวทางการปรับปรุงตลอดจนสร้างความแข็งแกร่งให้กับการควบคุมที่ช่วยป้องกันและตรวจพบความผิดพลาดของข้อมูล

การสร้างความตระหนักถึงความเสี่ยง

ความเสี่ยงทางตรงที่เกี่ยวข้องกับ GDPR คือ ค่าปรับที่อาจต้องจ่าย และผลกระทบด้านชื่อเสียง อย่างไรก็ตาม เมื่อพิจารณาลึกลงไปถึงจุดมุ่งหมายของกฎหมายฉบับนี้ ผู้ตรวจสอบภายในจะสามารถมองเห็นถึงความเสี่ยงอื่นๆ ที่เกี่ยวข้องกับการปกป้องข้อมูลด้วย

การติดตามดูแล การวัดผล และการรายงาน องค์กรต้องมี เจ้าหน้าที่ด้านการปกป้องข้อมูล (Data Protection Officer - DPO) เพื่อดำเนินการเกี่ยวกับความเป็นส่วนตัวและการปฏิบัติตามกฎหมายนี้ งานของ DPO รวมถึงการรายงานเกี่ยวกับการติดตามดูแลการปฏิบัติตาม

กฎหมาย การฝึกอบรมบุคลากร และการทำให้มั่นใจได้ว่า มีการตรวจสอบการปฏิบัติตามกฎหมายด้านความเป็นส่วนตัวนี้ องค์กรต้องทำการประเมินผลกระทบที่มีต่อความเป็นส่วนตัวของข้อมูล เมื่อมีการนำเทคโนโลยี หรือระบบงานใหม่ๆ มาใช้ ต้องมีการแจ้งให้ทราบภายในเวลาที่เหมาะสมเมื่อพบการละเมิดข้อมูล และต้องรายงานถึงการประมวลข้อมูลโดยบุคคลที่ 3 ด้วย

การป้องกันภัยอันตราย GDPR กำหนดบทลงโทษและค่าปรับสำหรับองค์กรที่ประมวลข้อมูลอย่างผิดกฎหมาย หรือไม่สามารถปกป้องข้อมูลได้ นอกจากนี้ แต่ละบุคคลอาจขอให้องค์กรนำข้อมูลส่วนตัวของตนเองออกจากระบบอัตโนมัติที่ใช้ประมวลและจัดการข้อมูลได้ด้วย

การจัดการเมื่อมีการละเมิด องค์กรต้องกำหนดกระบวนการในการแจ้งบุคคลต่างๆ ให้ทราบถึงการละเมิดข้อมูลภายใน 72 ชั่วโมงนับตั้งแต่พบการละเมิดนั้น หากองค์กรเห็นว่าการละเมิดนั้นจะก่อให้เกิดความเสี่ยงระดับสูงที่เป็นภัยต่อความเป็นส่วนตัวของบุคคลนั้นๆ

การเปิดกว้าง ความโปร่งใส และการแจ้งข้อมูล องค์กรต้องจัดเก็บข้อมูลเพื่อวัตถุประสงค์ที่เฉพาะเจาะจงและถูกต้องตามกฎหมาย และต้องแจ้งบุคคลต่างๆ ว่าองค์กรจะนำข้อมูลของพวกเขาไปใช้งานอย่างไร และต้องแจ้งถึงวิธีการปกป้องข้อมูลส่วนตัวเมื่อมีการส่งต่อไปยังประเทศที่ 3

การมีส่วนร่วมของแต่ละบุคคล ประชากรของ EU อาจขอเข้าถึงข้อมูลของตนเอง ขอสำเนาข้อมูล และขอยกเลิกการยินยอมให้ใช้ข้อมูลส่วนตัว หากว่าการขอยกเลิกนั้นไม่มีผลให้เกิดการฝ่าฝืนกฎหมาย แต่ละบุคคลยังอาจห้ามไม่ให้มีการใช้ข้อมูลของตนเองเพื่อการตลาดทางตรง และการจัดการข้อมูล และอาจติดต่อ DPO เมื่อมีประเด็นใดๆ เกี่ยวกับการประมวลข้อมูลส่วนตัวของตนเอง

ผู้ตรวจสอบภายในสามารถให้ความรู้แก่ฝ่ายจัดการเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้น และวิธีการบริหารความเสี่ยงในแต่ละเรื่องได้ และสามารถสื่อสารสารสนเทศที่เกี่ยวข้องกับความเสี่ยงเหล่านี้ โดยใช้จดหมายอิเล็คทรอนิคส์ที่ไม่เป็นทางการ จดหมายข่าวของหน่วยงาน หรือการประชุมร่วมกับฝ่ายจัดการ

การให้ความเชื่อมั่นต่อการปฏิบัติตามกฎหมาย

เมื่อใดที่นโยบาย และขั้นตอนการทำงานใหม่ๆ มีความสมบูรณ์มากขึ้น ผู้ตรวจสอบภายในจะต้องทำการตรวจสอบการปฏิบัติตาม GDPR อย่างเป็นประจำ เพื่อให้ทราบว่า องค์กรได้ปฏิบัติตาม GDPR มากน้อยเพียงใด ผู้ตรวจสอบควรให้ความสำคัญกับวิธีการที่องค์กรจัดการกับข้อมูลเพื่อช่วยสร้างความแข็งแกร่งให้กับการควบคุมด้านความเป็นส่วนตัว และความมั่นคงปลอดภัย และควรทำให้มั่นใจได้ว่า การควบคุมนั้น ถูกออกแบบอย่างเหมาะสม และมีการนำไปใช้อย่างมีประสิทธิผล ผู้ตรวจสอบยังต้องให้ความเชื่อมั่นต่อการปฏิบัติตามกฎหมายในประเด็นหลักๆ และต้องแจ้งเตือนปัญหาล่วงหน้าอีกด้วย

ทางเลือก และการให้ความยินยอม ภายใต้ GDPR องค์กรต้องอนุญาตให้ผู้ใช้งานระบบเลือกได้ว่า ข้อมูลส่วนตัวของพวกเขาจะถูกใช้งานอย่างไร และองค์กรต้องบันทึกและเก็บรักษาการให้ความยินยอมดังกล่าว รวมทั้งต้องขออนุญาตผู้ปกครองก่อนที่จะทำการเก็บข้อมูลของเยาวชน

เจตนารมณ์ของกฎหมาย เพื่อให้มั่นใจว่า การเก็บข้อมูลถูกต้องตามกฎหมายและมีความจำเป็น องค์กรสามารถเก็บเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต่อวัตถุประสงค์ที่กำหนดไว้ การทบทวนและการจัดการคำร้องที่ขอให้มีการประมวลข้อมูลเพิ่มเติม การยับยั้งคำร้องที่ขอข้อมูลเกี่ยวกับการลงโทษผู้กระทำผิด การบันทึกสถานการณ์ที่ไม่สามารถใช้สิทธิในการคัดค้านได้ ล้วนแล้วแต่เป็นเรื่องที่สำคัญ ทั้งนี้ ผู้ตรวจสอบภายในสามารถช่วยลดความเสี่ยงได้ โดยการสุ่มตรวจสอบวิธีการจัดเก็บข้อมูลเพื่อให้เป็นไปตามกฎหมาย

ข้อจำกัด องค์กรอาจจัดเก็บข้อมูลไว้ได้ภายในช่วงเวลาที่ไม่เกินกว่าวัตถุประสงค์ในการจัดเก็บข้อมูล และองค์กรต้องทำการลบข้อมูลส่วนตัวของแต่ละบุคคลเมื่อมีการร้องขอ แต่ GDPR อนุญาตให้องค์กรจัดเก็บข้อมูลอย่างถาวร เพื่อสาธารณประโยชน์ หรือเพื่อวัตถุประสงค์ทางการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ได้

การไหลเวียนอย่างอิสระของสารสนเทศ และข้อจำกัดทางกฎหมาย หลักการนี้รวมถึงการปกป้องคุ้มครองการถ่ายโอนข้อมูลที่ต้องเป็นไปตามข้อตกลงที่มีผลผูกพันตามกฎหมายระหว่างหน่วยงานของรัฐ กฎระเบียบของบริษัท ข้อสัญญามาตรฐาน และกลวิธีการทำงานอื่นๆ

การบริหารผู้รับจ้างที่เป็นบุคคลที่ 3 หลักการนี้ทำให้เกิดความมั่นใจว่า องค์กรต้องได้รับการประกันจากผู้รับจ้างว่า จะปฏิบัติตาม GDPR พร้อมด้วยหลักฐานว่าบุคคลที่ 3 นั้น มีการปกป้องคุ้มครองที่จำเป็น ทั้งด้านเทคนิค และด้านองค์กร ทั้งนี้ DPO ของผู้ควบคุมข้อมูล (ซึ่งหมายถึงบุคคลหรือองค์กรที่กำหนดวัตถุประสงค์และวิธีการในการประมวลข้อมูล) ต้องมีการอนุญาตอย่างเป็นลายลักษณ์อักษรเพื่อที่จะใช้ระบบการประมวลผลใดๆ ก็ตาม

ความรับผิดชอบ หลักความรับผิดชอบของ GDPR กำหนดหลักการพื้นฐานด้านกฎหมายในการประมวลข้อมูลส่วนบุคคล กำหนดบทบาทของ DPO และแจ้งต่อพลเมืองและผู้มีถิ่นพำนักใน EU ให้ทราบถึงสิทธิและการปกป้องคุ้มครองความเป็นส่วนตัว นอกเหนือจากการควบคุมดูแลกลยุทธ์ในการปกป้องข้อมูลแล้ว DPO ยังต้องติดต่อกับหน่วยงานที่ควบคุมดูแล และแสดงให้เห็นถึงการปฏิบัติตาม GDPR ด้วย

ผู้ตรวจสอบภายในจะต้องหมั่นประเมินกระบวนการและการควบคุมของแต่ละหลักการอย่างเป็นระยะ เพื่อให้มั่นใจได้ว่าการควบคุมได้ถูกออกแบบและนำไปใช้อย่างมีประสิทธิผล ผู้ตรวจสอบสามารถสอบทานตัวอย่างของเอกสารการถ่ายโอนข้อมูล เพื่อค้นหาข้อมูลที่ไม่ควรถูกถ่ายโอนไปยังองค์กรอื่น และสามารถเรียกดูรายงานเพื่อค้นหาข้อมูลที่ถูกจัดเก็บไว้นานเกินจำเป็น และสอบทานเอกสารที่มีอยู่เพื่อหาสิ่งผิดปกติอื่นๆ

แผนการตรวจสอบ GDPR

เพื่อเป็นการช่วยให้องค์กรถือปฏิบัติตาม GDPR ผู้ตรวจสอบภายในควรกำหนดแผนการตรวจสอบให้ครอบคลุมถึงการประเมิน GDPR อย่างเป็นอิสระ และการทดสอบว่ามีการปฏิบัติจริง ทั้งนี้ ผู้ตรวจสอบภายในสามารถสร้างความตระหนักถึงการไม่ปฏิบัติตาม GDPR ต่อผู้บริหารและคณะกรรมการ โดยการเน้นถึงการควบคุมที่ออกแบบไว้ไม่ดีหรือขาดหายไป และในที่สุด ผู้ตรวจสอบภายในสามารถสร้างโอกาสในการตรวจสอบกระบวนการที่หน่วยงานต่างๆ ใช้ร่วมกัน

ที่มา: https://iaonline.theiia.org/