GDPR และการส่งข้อความในระดับมืออาชีพ: ทำไมคนส่วนใหญ่ถึงละเมิดกฎโดยไม่รู้ตัว

เกือบทุกสำนักงาน คลินิก หรือบริษัทที่ปรึกษา ส่งเอกสารลูกค้าผ่านแอปพลิเคชันที่เซิร์ฟเวอร์ตั้งอยู่นอกเขตเศรษฐกิจยุโรป โดยไม่มีเจตนาร้าย แต่ในหลายกรณีถือเป็นการละเมิดกฎระเบียบโดยไม่มีใครเตือน

เอกสารที่เดินทางไปไกลกว่าที่คุณคิด

สถานการณ์ทั่วไป: ที่ปรึกษาภาษีได้รับเอกสารที่มีข้อมูลลูกค้าผ่านแอปส่งข้อความ พนักงานขายส่งต่อใบเสนอราคาให้เพื่อนร่วมงานผ่านแชท แพทย์แชร์รายงานการรักษาให้เพื่อนร่วมงานผ่านช่องทางเดียวกัน ไม่มีใครคิดซ้ำสอง มันเป็นเรื่องปกติ สะดวกสบาย และเป็นสิ่งที่ทำกันทุกวันในทุกสำนักงานในทุกเมืองของยุโรป

แต่ในหลายกรณี เอกสารนี้เพิ่งเดินทางไปยังเซิร์ฟเวอร์ในสหรัฐอเมริกา มันถูกจัดเก็บไว้ แม้จะชั่วคราว แม้จะมีการ "เข้ารหัสขณะจัดเก็บ" ก็ตาม ในคลาวด์ที่ทั้งมืออาชีพและลูกค้าไม่ได้ควบคุม มันผ่านระบบที่สามารถดึง Metadata ที่เกี่ยวข้องกับเนื้อหาออกมาทำดัชนีได้ในเชิงเทคนิค และระเบียบการคุ้มครองข้อมูลทั่วไปของยุโรปมีข้อกำหนดที่ค่อนข้างชัดเจนเกี่ยวกับเรื่องนี้

สิ่งที่ระเบียบข้อบังคับกำหนด

GDPR และแนวทางปฏิบัติของศาลยุติธรรมแห่งสหภาพยุโรป (โดยเฉพาะคำตัดสิน Schrems II, C-311/18 ในปี 2020) กำหนดว่าข้อมูลส่วนบุคคลของพลเมืองยุโรปต้องได้รับการคุ้มครองอย่างเหมาะสม หากข้อมูลนี้ออกนอกเขตเศรษฐกิจยุโรป ผู้ควบคุมข้อมูลต้องรับประกันว่าผู้รับมีระดับการคุ้มครองที่ "เทียบเท่าอย่างเป็นสาระสำคัญ" กับของยุโรป ในเชิงปฏิบัติ การส่งข้อมูลลูกค้าผ่านบริการที่มีเซิร์ฟเวอร์อยู่ภายใต้เขตอำนาจศาลของสหรัฐฯ โดยไม่มีการประเมินผลกระทบและไม่มีการดำเนินมาตรการรับประกันเพิ่มเติม เช่น ข้อสัญญามาตรฐาน มาตรการทางเทคนิคเสริม เช่น การเข้ารหัสที่ตรวจสอบได้ ฯลฯ อาจถือเป็นการละเมิดกฎระเบียบได้ แม้ว่าจนถึงตอนนี้จะยังไม่มีใครทักท้วงก็ตาม

และไม่ใช่เพียงแค่เรื่องเนื้อหาของข้อความเท่านั้น Metadata เช่น ใครส่งอะไรให้ใคร เมื่อไหร่ บ่อยแค่ไหน จากที่ไหน ก็เป็นข้อมูลส่วนบุคคลตามกฎระเบียบ ตามการตีความซ้ำๆ ของคณะกรรมการคุ้มครองข้อมูลแห่งยุโรป บริการที่รวบรวม Metadata จากการสื่อสารทางวิชาชีพของผู้ใช้กำลังประมวลผลข้อมูลส่วนบุคคลของลูกค้าของผู้ใช้รายนั้น โดยที่พวกเขาไม่รับรู้หรือไม่ได้ให้ความยินยอมสำหรับการประมวลผลดังกล่าว

แนวคิดทั่วไปที่ว่า "ฉันใช้แอปเพื่อเขียนเท่านั้น แอปไม่ใช่ผู้จัดเก็บข้อมูลของลูกค้าฉัน" นั้นผิดในแง่กฎหมาย หากข้อมูลลูกค้าผ่านโครงสร้างพื้นฐานของบุคคลภายนอก บุคคลภายนอกนั้นกำลังประมวลผลข้อมูลเหล่านั้น และหากมีการ

ประมวลผล ก็ต้องมีฐานอำนาจทางกฎหมาย สัญญาการประมวลผลข้อมูล และมาตรการรับประกันที่เหมาะสม

ใครคือผู้รับผิดชอบ

คำถามที่ว่าใครเป็นผู้รับผิดชอบทางกฎหมายไม่ใช่คำถามเชิงวิชาการ GDPR แยกความแตกต่างระหว่าง *ผู้ควบคุมข้อมูล* (ผู้ตัดสินใจว่าข้อมูลใดจะถูกประมวลผลและเพื่อวัตถุประสงค์ใด) และ *ผู้ประมวลผลข้อมูล* (ผู้ดำเนินการในนามของผู้ควบคุม) มืออาชีพที่ส่งเอกสารลูกค้าคือผู้ควบคุมข้อมูล ผู้ให้บริการแอปส่งข้อความในหลายกรณีคือผู้ประมวลผลข้อมูลตามพฤตินัย หากไม่มีสัญญาการประมวลผลข้อมูล และไม่มีข้อกำหนดส่วนใหญ่ที่สัญญาดังกล่าวควรมี ผู้ควบคุมข้อมูลก็ถือว่าไม่ได้ทำตามหน้าที่

การตีความแบบผ่อนปรนบอกว่า "มืออาชีพส่วนใหญ่ไม่รู้เรื่องนี้" การตีความแบบเคร่งครัดบอกว่า "การไม่รู้กฎหมายไม่ใช่ข้อแก้ตัว" และการตีความของทนายความผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลทุกคนที่ให้ความเห็นในเรื่องนี้ มักจะเป็นการตีความแบบเคร่งครัด

เรื่องนี้สำคัญกับใครในทางปฏิบัติ

สำหรับมืออาชีพหรือบริษัททุกคนที่ต้องจัดการกับข้อมูลส่วนบุคคลของบุคคลภายนอก แม้เพียงเป็นครั้งคราว:

- ทนายความที่ได้รับเอกสารของลูกค้า (สัญญา, คำฟ้อง, คำแถลง, รายงานทรัพย์สิน)
- แพทย์และบุคลากรทางการแพทย์อื่นๆ ที่แชร์ข้อมูลสุขภาพ ซึ่งถือเป็น *ข้อมูลประเภทพิเศษ* ตามมาตรา 9 ของ GDPR ที่มีระบบการคุ้มครองที่เข้มงวดเป็นพิเศษ
- ที่ปรึกษาภาษีและผู้จัดการฝ่ายบริหารที่จัดการข้อมูลระบุตัวตน ภาษี และธนาคาร
- แผนกทรัพยากรบุคคลที่จัดการเอกสารการทำงานและข้อมูลส่วนตัวของพนักงาน
- ตัวแทนฝ่ายขายที่ได้รับรายละเอียดการติดต่อและข้อมูลธุรกิจที่ละเอียดอ่อนจากผู้มุ่งหวังและลูกค้า

ในทุกกรณี ข้อมูลจะได้รับความคุ้มครองโดย GDPR ในทุกกรณีตามแนวปฏิบัติทั่วไป ข้อมูลเหล่านี้ไหลผ่านช่องทางที่เขตอำนาจศาลไม่อนุญาตให้ประกาศว่า "เทียบเท่าอย่างเป็นสาระสำคัญ" กับกรอบการทำงานของยุโรปโดยไม่มีมาตรการรับประกันเพิ่มเติม ไม่ใช่เพราะเจตนาร้าย แต่เกิดจากความเคยชิน และเกิดจากโครงสร้างพื้นฐานทางเทคโนโลยีที่ให้ความสำคัญกับความสะดวกสบายมากกว่าการปฏิบัติตามกฎเกณฑ์มาตลอดสิบห้าปี

ข้อโต้แย้งที่ว่า "ใครๆ ก็ทำกัน"

เราควรคาดการณ์ถึงข้อคัดค้านที่พบบ่อยที่สุด: "ถ้าทุกคนทำเหมือนกันหมด มันก็ไม่น่าจะเป็นปัญหาจริงๆ" นี่เป็นข้อโต้แย้งที่เข้าใจได้ในความรู้สึก แต่ไม่มีผลในทางกฎหมาย ความจริงที่ว่าแนวปฏิบัติหนึ่งแพร่หลายไม่ได้ทำให้มันสอดคล้องกับกฎระเบียบ หน่วยงานคุ้มครองข้อมูลได้สั่งลงโทษบริษัทหลายแห่งในช่วงไม่กี่ปีที่ผ่านมา เนื่องจากรูปแบบการใช้การส่งข้อความที่ดูเหมือนไม่มีอันตรายจนกระทั่งถึงเวลาตรวจสอบ

ความเป็นจริงในการดำเนินงานปัจจุบันคือ ความเสี่ยงในเชิงโอกาสนั้นต่ำ เพราะนานๆ ครั้งที่หน่วยงานจะตรวจสอบเครื่องมือส่งข้อความเฉพาะทางของสำนักงานขนาดกลาง แต่มีความเสี่ยงสูงในเชิงผลกระทบหากเกิดขึ้นจริง เป็นความเสี่ยงที่คนส่วนใหญ่แบกรับโดยไม่รู้ตัวว่ากำลังแบกรับอยู่ นั่นคือการไม่ได้ประเมินว่าเครื่องมือที่ใช้สอดคล้องกับความรับผิดชอบทางกฎหมายของผู้ควบคุมข้อมูลหรือไม่

ร่องรอยดิจิทัลมีผลย้อนหลัง

มีข้อโต้แย้งประการที่สองที่เกือบจะสมมาตรกับข้อก่อนหน้าซึ่งควรคาดการณ์ไว้: *"ถ้าเรื่องนี้เป็นปัญหาร้ายแรง ฝ่ายบริหารก็คงเริ่มเข้ามาควบคุมดูแลแล้ว"* ความเป็นจริงที่สังเกตได้ในปัจจุบันทำให้ข้อโต้แย้งนี้ดูมีน้ำหนักในเบื้องต้น การตรวจสอบเนื่องจากการใช้การส่งข้อความอย่างไม่เหมาะสมในบริษัทขนาดเล็กและโดยเฉพาะในกลุ่มฟรีแลนซ์แทบจะไม่มีให้เห็นในวันนี้ ไม่ใช่เพราะพฤติกรรมดังกล่าวได้รับอนุญาต แต่เป็นเพราะหน่วยงานในหลายพื้นที่ขาดแคลนทรัพยากรบุคคลที่จำเป็นในการตรวจสอบกิจการหลายล้านแห่ง

นั่นคือสิ่งที่แนวปฏิบัติที่สังเกตได้ในวันนี้บ่งบอก แต่นั่นไม่ใช่สิ่งที่ทศวรรษหน้าบ่งบอก สองปัจจัยกำลังบรรจบกันเพื่อเปลี่ยนสมดุลในระยะเวลาอันสั้น

ประการแรก: ร่องรอยดิจิทัลมีผลย้อนหลัง ทุกข้อความที่ส่งผ่านแอปพลิเคชันที่มีเซิร์ฟเวอร์ส่วนกลางจะยังคงถูกบันทึกไว้ อย่างน้อยก็ใน Metadata ภายในโครงสร้างพื้นฐานที่ยังคงอยู่ สิ่งที่ส่งไปเมื่อหกเดือนก่อนในทางเทคนิคแล้วยังสามารถตรวจสอบได้ในวันนี้ สิ่งที่ส่งวันนี้ก็จะสามารถตรวจสอบได้ในอีกห้าปีข้างหน้า การไม่มีการตรวจสอบในปัจจุบันไม่ใช่การรับประกันว่าจะไม่มีการตรวจสอบในอนาคต มันคือการเลื่อนการประเมินออกไป ไม่ใช่การได้รับการยกเว้น

ประการที่สอง: ความสามารถในการตรวจสอบทางปกครองจะเติบโตอย่างก้าวกระโดด การนำเครื่องมือปัญญาประดิษฐ์มาใช้ในกระบวนการควบคุมจะกำจัดคอขวดด้านบุคลากรที่เคยปกป้องบริษัทขนาดเล็กและฟรีแลนซ์ไว้ ระบบที่สามารถตรวจสอบข้อมูลข้ามกันระหว่าง Metadata มหาศาล การยื่นภาษี ทะเบียนพาณิชย์ และหน้าที่ในการแจ้งเหตุละเมิดความปลอดภัย ไม่ต้องการผู้ตรวจการ แต่ต้องการการเข้าถึง และการเข้าถึงผ่านข้อกำหนดที่ส่งไปยังผู้ให้บริการที่มีตัวตนทางกฎหมายในยุโรปภายใต้กรอบระเบียบปัจจุบันนั้นสามารถทำได้จริง

นอกจากนี้ยังมีปัจจัยที่ไม่ใช่เชิงเทคนิคแต่สำคัญไม่แพ้กัน นั่นคือประเทศในยุโรปกำลังอยู่ในกระบวนการก่อหนี้เพิ่มขึ้นอย่างต่อเนื่อง และเกือบทุกประเทศจำเป็นต้องขยายฐานภาษีของตน การลงโทษทางปกครองที่เกิดจากการไม่ปฏิบัติตาม GDPR ในเชิงการคลังล้วนๆ คือแหล่งรายได้ที่กำลังเติบโตและมีความสะดวกทางการเมือง นี่ไม่ใช่การคาดเดา แต่เป็นแนวโน้มที่สังเกตได้ในรายงานประจำปีของหน่วยงานคุ้มครองข้อมูลในยุโรป ซึ่งมียอดรวมของค่าปรับเพิ่มขึ้นติดต่อกันหลายปีงบประมาณ

ข้อสรุปเชิงปฏิบัติการสำหรับผู้ควบคุมข้อมูลไม่ใช่การสร้างความตระหนกแต่เป็นการมองโลกตามความเป็นจริง: **การตัดสินใจเกี่ยวกับวิธีจัดการการสื่อสารกับลูกค้าในปัจจุบัน จะถูกประเมินเทียบกับความสามารถในการตรวจสอบของปีที่มีการตรวจสอบ ไม่ใช่เทียบกับความสามารถในปัจจุบัน** และความสามารถนั้นในระยะเวลาที่เหมาะสมจะแตกต่างจากวันนี้อย่างสิ้นเชิง ใครที่เริ่มทำสิ่งที่ถูกต้องตั้งแต่วันนี้จะไม่เพียงแค่ถูกต้องตั้งแต่วันนี้เท่านั้น แต่ร่องรอยที่เกิดขึ้นตั้งแต่วินาทีนี้จะสอดคล้องกับระเบียบข้อบังคับ และนั่นช่วยปกป้องช่วงเวลาที่จะมาถึงย้อนหลัง ใครที่ยังคงทำแบบเดิมต่อไปก็จะสะสมร่องรอยที่ตรวจสอบได้ซึ่งความสอดคล้องจะถูกประเมินตามมาตรฐานและทรัพยากรของปีต่อๆ ไป

อะไรจะเปลี่ยนไปหากใช้สถาปัตยกรรมที่แตกต่าง

มีทางเลือกทางเทคนิคที่ข้อมูลไม่ได้ถูกเก็บไว้ในโครงสร้างพื้นฐานของบุคคลภายนอก แต่จะเดินทางจากอุปกรณ์ของผู้ส่งไปยังผู้รับโดยตรง ในสถาปัตยกรรมนี้ การปฏิบัติตาม GDPR ในส่วนที่เกี่ยวกับการโอนย้ายข้อมูลระหว่างประเทศจะไม่ขึ้นอยู่กับข้อสัญญามาตรฐาน ไม่ขึ้นอยู่กับความปรารถนาดีของผู้ให้บริการ และไม่ขึ้นอยู่กับการตรวจสอบในอนาคต มันขึ้นอยู่กับข้อเท็จจริงที่ว่า *ไม่มีการโอนย้ายข้อมูลเกิดขึ้น* และสิ่งใดที่ไม่มีอยู่จริงย่อมไม่สามารถถูกละเมิดได้

นี่ไม่ใช่ทางออกเดียวและไม่ใช่ทางออกเดียวที่เป็นไปได้ แต่มันแตกต่างในเชิงโครงสร้าง และการปฏิบัติตามระเบียบข้อบังคับจะไม่ใช่เพียงส่วนเสริมของกระบวนการอีกต่อไป แต่จะกลายเป็นผลลัพธ์โดยตรงจากการออกแบบ สำหรับมืออาชีพที่ให้ความสำคัญกับความรับผิดชอบในฐานะผู้ควบคุมข้อมูล ความแตกต่างนี้คือสิ่งสำคัญ

ฉบับหน้าของ Cuadernos จะวิเคราะห์รายละเอียดเกี่ยวกับคำตัดสิน Schrems II และผลกระทบเชิงปฏิบัติสำหรับวิสาหกิจขนาดกลางและขนาดย่อมที่พึ่งพาบริการคลาวด์ของสหรัฐฯ ในช่วงห้าปีหลังการประกาศใช้

แหล่งข้อมูลและกรอบระเบียบข้อบังคับ

- ระเบียบ (EU) 2016/679 (GDPR) โดยเฉพาะบทที่ 5 เกี่ยวกับการโอนย้ายข้อมูลระหว่างประเทศ
- ศาลยุติธรรมแห่งสหภาพยุโรป C-311/18 ("Schrems II"), 16 กรกฎาคม 2020
- EDPB – คำแนะนำ 01/2020 เกี่ยวกับมาตรการเสริมสำหรับเครื่องมือในการโอนย้ายข้อมูล
- หน่วยงานคุ้มครองข้อมูล – รายงานประจำปีพร้อมกรณีศึกษาการลงโทษเนื่องจากการใช้การส่งข้อความทันทีอย่างไม่เหมาะสมในสภาพแวดล้อมทางวิชาชีพ

← ก่อนหน้าความลับในวิชาชีพในยุคดิจิทัลถัดไป → เมื่อไม่มีใครอยู่ตรงกลาง

บทความล่าสุด

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

↓ Markdown ↓ ข้อความธรรมดา ↓ PDF

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั่ง · SHA-256 998bb7de9b1c8950cc07b155c250456ad5a3a5f95fbfa1237f8d2f2a5fca76e6

Cuadernos Lacre · สิ่งพิมพ์ของ Menzuri Gestión S.L. ·
เขียนโดย R.Eugenio · เรียบเรียงโดยทีมงาน Solo2