GDPR और पेशेवर संदेश सेवा: क्यों अधिकांश लोग अनजाने में नियमों का उल्लंघन करते हैं

लगभग हर कार्यालय, क्लिनिक या परामर्श फर्म मैसेजिंग ऐप के माध्यम से क्लाइंट दस्तावेज़ भेजती है जिनका सर्वर यूरोपीय आर्थिक क्षेत्र के बाहर स्थित होता है। बिना किसी बुरी नियत के, लेकिन कई मामलों में विनियमन का उल्लंघन करते हुए और बिना किसी चेतावनी के।

दस्तावेज़ जो आपकी सोच से कहीं अधिक दूर तक यात्रा करता है

एक रोज़मर्रा की स्थिति: एक कर सलाहकार संदेश के माध्यम से क्लाइंट डेटा वाला दस्तावेज़ प्राप्त करता है। एक सेल्समैन चैट के माध्यम से किसी सहयोगी को प्रस्ताव भेजता है। एक डॉक्टर उसी तरह किसी सहयोगी के साथ नैदानिक रिपोर्ट साझा करता है। कोई दो बार नहीं सोचता। यह सामान्य है। यह सुविधाजनक है। यह यूरोप के हर शहर के हर कार्यालय में हर दिन किया जाता है।

लेकिन यह दस्तावेज़, कई मामलों में, अभी-अभी संयुक्त राज्य अमेरिका के एक सर्वर पर गया है। इसे संग्रहीत किया गया था – भले ही अस्थायी रूप से, भले ही "एन्क्रिप्टेड" रूप में – एक क्लाउड में जिसे न तो पेशेवर और न ही उसका क्लाइंट नियंत्रित करता है। यह उन प्रणालियों से गुज़रा है जो तकनीकी रूप से सामग्री से जुड़े मेटाडेटा को अनुक्रमित कर सकते हैं। और यूरोपीय सामान्य डेटा सुरक्षा विनियमन के पास इस बारे में काफी स्पष्ट बातें हैं।

मानक की आवश्यकताएं

GDPR – और इसके परिणामस्वरूप यूरोपीय संघ के न्यायालय का न्यायशास्त्र (विशेष रूप से 2020 का Schrems II निर्णय, C-311/18) – निर्धारित करता है कि यूरोपीय नागरिकों के व्यक्तिगत डेटा को उचित रूप से संरक्षित किया जाना चाहिए। यदि यह डेटा यूरोपीय आर्थिक क्षेत्र को छोड़ देता है, तो डेटा नियंत्रक को यह गारंटी देनी चाहिए कि प्राप्तकर्ता यूरोपीय के "अनिवार्य रूप से समकक्ष" सुरक्षा स्तर प्रदान करता है। व्यवहार में, इसका मतलब यह है कि उन सेवाओं के माध्यम से क्लाइंट डेटा भेजना जिनके सर्वर अमेरिकी अधिकार क्षेत्र के अधीन हैं, बिना प्रभाव मूल्यांकन किए और बिना पूरक गारंटी लागू किए – मानक संविदात्मक खंड, सत्यापन योग्य एन्क्रिप्शन जैसे अतिरिक्त तकनीकी उपाय आदि – विनियमन का उल्लंघन हो सकता है। भले ही अभी तक किसी ने कुछ न कहा हो।

और बात सिर्फ संदेशों की सामग्री की नहीं है। विनियमों के अनुसार और यूरोपीय डेटा सुरक्षा बोर्ड की बार-बार की व्याख्या के अनुसार, मेटाडेटा – कौन किसे क्या भेजता है, कब, कितनी बार, कहाँ से – भी व्यक्तिगत डेटा है। एक सेवा जो उपयोगकर्ता के पेशेवर संचार से मेटाडेटा एकत्र करती है, वह उस उपयोगकर्ता के ग्राहकों के व्यक्तिगत डेटा को संसाधित करती है, बिना उनकी जानकारी के या इस तरह के प्रसंस्करण के लिए कोई सहमति दिए बिना।

आम विचार योजना – "मैं केवल लिखने के लिए ऐप का उपयोग करता हूं; ऐप मेरे क्लाइंट का डेटा प्रदाता नहीं है" – कानूनी रूप से गलत है। यदि क्लाइंट का डेटा किसी तीसरे पक्ष के बुनियादी ढांचे से गुज़रता है, तो वह तीसरा पक्ष उस डेटा को संसाधित कर रहा है। और यदि वह इसे संसाधित करता है, तो एक कानूनी आधार, एक डेटा प्रसंस्करण अनुबंध और उचित गारंटी होनी चाहिए।

ज़िम्मेदार कौन है

कानूनी जिम्मेदारी कौन उठाता है यह सवाल अकादमिक नहीं है। GDPR *डेटा नियंत्रक* (जो तय करता है कि कौन सा डेटा किस उद्देश्य के लिए संसाधित किया जाता है) और *डेटा संसाधक* (जो नियंत्रक की ओर से सामग्री के रूप में ऐसा करता है) के बीच अंतर करता है। क्लाइंट दस्तावेज़ भेजने वाला पेशेवर डेटा नियंत्रक है। मैसेजिंग ऐप प्रदाता कई मामलों में वास्तविक डेटा संसाधक है। प्रसंस्करण अनुबंध के बिना – और बिना अधिकांश खंडों के जो इस तरह के अनुबंध में होने चाहिए – नियंत्रक ने अपने दायित्व को पूरा नहीं किया है।

उदार व्याख्या कहती है: "अधिकांश पेशेवर इसे नहीं जानते हैं"। सख्त व्याख्या कहती है: "कानून की अज्ञानता कोई बहाना नहीं है"। और इस संबंध में परामर्श किए गए किसी भी विशेषज्ञ डेटा सुरक्षा वकील की व्याख्या आमतौर पर सख्त होती है।

यह ठोस रूप से किसके लिए महत्वपूर्ण है

प्रत्येक पेशेवर या कंपनी के लिए जो कभी-कभार ही सही, तीसरे पक्ष की व्यक्तिगत जानकारी के साथ काम करती है:

- वकील जो क्लाइंट दस्तावेज़ प्राप्त करते हैं (अनुबंध, मुकदमे, घोषणाएँ, संपत्ति रिपोर्ट)।
- डॉक्टर और अन्य स्वास्थ्य पेशेवर जो स्वास्थ्य डेटा साझा करते हैं – जिन्हें GDPR के अनुच्छेद 9 के तहत मजबूत सुरक्षा व्यवस्था के साथ *विशेष श्रेणियों* के रूप में माना जाता है –।
- कर सलाहकार और प्रशासनिक प्रबंधक जो पहचान, कर और बैंक डेटा के साथ काम करते हैं।
- मानव संसाधन विभाग जो कर्मचारियों के काम और व्यक्तिगत दस्तावेज़ों का प्रबंधन करते हैं।
- वाणिज्यिक प्रतिनिधि जो संभावित और मौजूदा ग्राहकों से संपर्क विवरण और अक्सर संवेदनशील व्यावसायिक जानकारी प्राप्त करते हैं।

सभी मामलों में जानकारी GDPR द्वारा सुरक्षित है। सभी मामलों में, सामान्य व्यवहार में, यह जानकारी उन चैनलों के माध्यम से बहती है जिनका अधिकार क्षेत्र अतिरिक्त गारंटी के बिना उन्हें यूरोपीय ढांचे के "अनिवार्य रूप से समकक्ष" घोषित करने की अनुमति नहीं देता है। किसी बुरी नियत से नहीं। आदत से। और एक तकनीकी बुनियादी ढांचे के कारण जिसने पंद्रह वर्षों तक सुविधा को अनुपालन से ऊपर रखा।

"सब कर रहे हैं" तर्क

सबसे आम आपत्ति का अनुमान लगाना समझदारी है: "यदि हर कोई ऐसा कर रहा है, तो यह वास्तविक समस्या नहीं हो सकती है"। यह पूरी तरह से समझने योग्य तर्क है और कानूनी रूप से इसका कोई बल नहीं है। तथ्य यह है कि एक व्यवहार व्यापक है, इसे विनियमन के अनुरूप नहीं बनाता है। डेटा सुरक्षा अधिकारियों ने हाल के वर्षों में कई कंपनियों को ठीक उन मैसेजिंग उपयोगों के लिए दंडित किया है जो निरीक्षण के क्षण तक हानिरहित लग रहे थे।

वर्तमान परिचालन वास्तविकता यह है कि संभावना के मामले में जोखिम कम है – यह बहुत दुर्लभ है कि प्राधिकरण का निरीक्षण एक मध्यम आकार के कार्यालय के विशिष्ट मैसेजिंग उपकरणों का ऑडिट करे – लेकिन प्रभाव के मामले में उच्च है यदि यह साकार होता है। यह एक ऐसा जोखिम है जिसे अधिकांश लोग यह जाने बिना लेते हैं कि वे इसे ले रहे हैं। यानी, यह मूल्यांकन किए बिना कि उपयोग किया गया उपकरण डेटा नियंत्रक की कानूनी जिम्मेदारी के अनुरूप है या नहीं।

डिजिटल पदचिह्न पूर्वव्यापी (retroactive) होते हैं

एक दूसरा तर्क है, जो पिछले वाले के लगभग सममित है, जिसका पूर्वानुमान लगाया जाना चाहिए: *"यदि यह एक गंभीर समस्या होती, तो प्रशासन पहले ही इसकी निगरानी करना शुरू कर देता"*। वर्तमान में देखी गई वास्तविकता उसे सतही तौर पर सही मानती है। छोटी कंपनियों और विशेष रूप से स्व-नियोजित लोगों में मैसेजिंग के अनुचित उपयोग के कारण निरीक्षण आज लगभग नगण्य हैं – इसलिए

नहीं कि व्यवहार की अनुमति है, बल्कि इसलिए कि यूरोप के बड़े हिस्से में प्रशासन के पास लाखों संस्थाओं का ऑडिट करने के लिए आवश्यक मानव संसाधनों की कमी है।

आज जो व्यवहार देखा गया है वह यही संकेत देता है। लेकिन आने वाला दशक यह संकेत नहीं दे रहा है। दो कारक अपेक्षाकृत कम समय के भीतर संतुलन को बदलने के लिए एकत्रित हो रहे हैं।

पहला: डिजिटल पदचिह्न पूर्वव्यापी होते हैं। केंद्रीय सर्वर वाले एप्लिकेशन के माध्यम से भेजा गया प्रत्येक संदेश कम से कम मेटाडेटा में, उस बुनियादी ढांचे में पंजीकृत रहता है जो बना रहता है। जो छह महीने पहले भेजा गया था वह तकनीकी रूप से आज भी ऑडिट योग्य है। आज जो भेजा जा रहा है वह पांच साल बाद भी ऑडिट योग्य होगा। वर्तमान में निरीक्षण की अनुपस्थिति भविष्य में निरीक्षण की अनुपस्थिति की गारंटी नहीं है। यह मूल्यांकन का विलंब है, छूट नहीं।

दूसरा: प्रशासनिक ऑडिट क्षमता तेजी से बढ़ेगी। नियंत्रण प्रक्रियाओं में कृत्रिम बुद्धिमत्ता उपकरणों की शुरूआत उस मानवीय बाधा को समाप्त कर देती है जिसने अब तक – वास्तव में, कानूनी रूप से नहीं – छोटी कंपनियों और स्व-नियोजित लोगों की रक्षा की है। बड़े पैमाने पर मेटाडेटा, टैक्स रिटर्न, वाणिज्यिक रजिस्टर और सुरक्षा उल्लंघन अधिसूचना दायित्वों को क्रॉस-रेफरेंस करने में सक्षम सिस्टम को निरीक्षकों की आवश्यकता नहीं होती है: उसे पहुंच की आवश्यकता होती है। और वर्तमान नियामक ढांचे के भीतर यूरोपीय संघ में कानूनी उपस्थिति वाले प्रदाताओं के लिए अनुरोधों के माध्यम से पहुंच पूरी तरह से संभव है।

इसमें एक कम तकनीकी लेकिन समान रूप से निर्णायक कारक जोड़ा गया है: यूरोपीय राज्य लगातार बढ़ते ऋण की प्रक्रिया में हैं और उन्हें लगभग बिना किसी अपवाद के अपने टैक्स आधार का विस्तार करने की आवश्यकता है। GDPR का पालन न करने से उत्पन्न प्रशासनिक दंड, शुद्ध वित्तीय संदर्भ में, एक बढ़ता हुआ और राजनीतिक रूप से सुविधाजनक आय का स्रोत है। यह कोई अनुमान नहीं है: यह यूरोपीय डेटा सुरक्षा अधिकारियों की वार्षिक रिपोर्ट में एक देखने योग्य प्रवृत्ति है, जहाँ दंड की कुल मात्रा लगातार कई वित्तीय वर्षों से बढ़ रही है।

डेटा नियंत्रक के लिए परिचालन निष्कर्ष डराने वाला नहीं बल्कि गंभीर है: **आज ग्राहकों के साथ संचार को कैसे प्रबंधित किया जाता है, इस निर्णय का मूल्यांकन उस वर्ष की निरीक्षण क्षमता के आधार पर किया जाता है जिसमें निरीक्षण होता है, न कि वर्तमान क्षमता के आधार पर।** और वह क्षमता उचित समय के भीतर आज की तुलना में काफी अलग होगी। जो आज चीजों को सही ढंग से करना शुरू करता है वह न केवल आज से ठीक रहेगा: इस क्षण से उत्पन्न पदचिह्न मानक के अनुरूप होंगे, और यह आने वाली अवधि को पूर्वव्यापी रूप से सुरक्षित करता है। जो पहले की तरह जारी रहेगा वह एक ऑडिट योग्य पदचिह्न जमा करेगा जिसका अनुपालन आने वाले वर्षों के मानकों – और संसाधनों – के आधार पर मूल्यांकित किया जाएगा।

एक अलग वास्तुकला के साथ क्या बदलता है

तकनीकी विकल्प मौजूद हैं जहाँ डेटा तीसरे पक्ष के बुनियादी ढांचे में संग्रहीत नहीं होता है, बल्कि सीधे भेजने वाले के डिवाइस से प्राप्तकर्ता के डिवाइस पर जाता है। इस वास्तुकला में, अंतर्राष्ट्रीय हस्तांतरण के संबंध में GDPR का अनुपालन मानक संविदात्मक खंडों पर, न ही प्रदाता की सद्भावना पर और न ही भविष्य के ऑडिट पर निर्भर करता है। यह इस बात पर निर्भर करता है कि *कोई हस्तांतरण नहीं है*। और जिसका अस्तित्व नहीं है उसका उल्लंघन नहीं किया जा सकता है।

यह एकमात्र समाधान नहीं है और न ही एकमात्र संभव है। लेकिन यह संरचनात्मक रूप से अलग है, और नियामक अनुपालन एक प्रक्रियात्मक परिशिष्ट होना बंद कर देता है और डिज़ाइन का सीधा परिणाम बन जाता है। एक पेशेवर के लिए जो डेटा नियंत्रक के रूप में अपनी जिम्मेदारी को गंभीरता से लेता है, यह अंतर मायने रखता है।

Cuadernos का अगला अंक Schrems II के फैसले और अमेरिकी क्लाउड सेवाओं पर निर्भर छोटे और मध्यम उद्यमों के लिए इसके व्यावहारिक निहितार्थों का विस्तार से विश्लेषण करेगा, इसके प्रकाशन के पांच साल बाद।

स्रोत और विनियामक ढांचा

- विनियमन (EU) 2016/679 (GDPR), विशेष रूप से अंतर्राष्ट्रीय हस्तांतरण से संबंधित अध्याय V।

- CJUE C-311/18 ("Schrems II"), 16 जुलाई, 2020।
- EDPB – हस्तांतरण उपकरणों के पूरक उपायों पर सिफारिशें 01/2020।
- डेटा सुरक्षा अधिकारी – पेशेवर वातावरण में इंस्टेंट मैसेजिंग के अनुचित उपयोग के कारण दंड के मामलों वाली वार्षिक रिपोर्ट।

← पिछलाडिजिटल युग में पेशेवर गोपनीयताअगला →जब बीच में कोई न हो

हाल की रीडिंग

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

इस लेख को अपने साथ ले जाएं जहाँ भी आपको इसकी आवश्यकता हो।

↓ मार्कडाउन ↓ सादा टेक्स्ट ↓ PDF

फ़ाइल आपके डिवाइस पर डाउनलोड हो जाएगी। वहां से आप इसे सहेज सकते हैं, Solo2 में आयात कर सकते हैं या जहां चाहें साझा कर सकते हैं। Cuadernos आपके लिए गंतव्य तय नहीं करता है।

मोहरबंद · SHA-256 0f176d33ecd7533aa8218a48f63e28c6b1d49138b838673f8298ffa712fd4b54

Cuadernos Lacre · Menzuri Gestión S.L. का एक प्रकाशन ·
R.Eugenio द्वारा लिखित · Solo2 की टीम द्वारा संपादित।