GDPR والمراسلات المهنية: لماذا ينتهك معظم الناس القواعد دون علمهم

يقوم كل مكتب أو عيادة أو شركة استشارية تقريبًا بإرسال مستندات العملاء عبر تطبيقات يقع خادمها خارج المنطقة الاقتصادية الأوروبية. دون نية سيئة، ولكن في كثير من الحالات ينتهكون اللائحة دون أن يحذرهم أحد.

ببساطة: ترسل لك مستشارتك الضريبية وثيقة عبر WhatsApp. تصل إلى هاتفك في مدريد، لكنها مرت قبل ذلك عبر خادم في تكساس. الـ GDPR لديه شيء واضح تمامًا ليقوله عن ذلك — ومعظم المكاتب تواصل انتهاكه منذ سنوات دون علمها.

المستند الذي يسافر أبعد مما تعتقد

موقف يومي: مستشار ضريبي يتلقى عبر المراسلة مستندًا يحتوي على بيانات عميل. بائع يوجه عبر الدردشة عرضًا لزميل. طبيبة تشارك بنفس الطريقة تقريرًا سريريًا مع زميل. لا أحد يفكر مرتين. إنه أمر طبيعي. إنه مريح. إنه ما يتم فعله كل يوم في كل مكتب في كل مدينة في أوروبا.

لكن هذا المستند، في كثير من الحالات، سافر للتو إلى خادم في الولايات المتحدة. تم تخزينه – ولو مؤقتًا، ولو "مشفرًا أثناء السكون" – في سحابة لا يتحكم فيها المهني ولا عميله. لقد مر عبر أنظمة يمكنها تقنيًا فهرسة البيانات الوصفية المرتبطة بالمحتوى. ولائحة حماية البيانات العامة الأوروبية لديها ما تقوله بوضوح تام حول هذا الموضوع.

ما تتطلبه القاعدة

تحدد GDPR – وبالتبعية اجتهادات محكمة العدل التابعة للاتحاد الأوروبي (خاصة حكم Schrems II، C-311/18، لعام 2020) – وجوب حماية البيانات الشخصية للمواطنين الأوروبيين بشكل مناسب. إذا غادرت هذه البيانات المنطقة الاقتصادية الأوروبية، يجب على المسؤول عن البيانات ضمان أن المتلقي يقدم مستوى من الحماية "يعادل في جوهره" المستوى الأوروبي. في الممارسة العملية، هذا يعني أن إرسال بيانات العملاء عبر خدمات تخضع خوادمها لولاية قضائية أمريكية، دون إجراء تقييم للأثر ودون تنفيذ ضمانات تكميلية – بنود تعاقدية قياسية، تدابير تقنية إضافية مثل التشفير القابل للتحقق، وما إلى ذلك – يمكن أن يشكل انتهاكًا للائحة. حتى لو لم يقل أحد أي شيء حتى الآن.

والأمر لا يتعلق فقط بمحتوى الرسائل. البيانات الوصفية – من يرسل ماذا لمن، متى، كم مرة، ومن أين – هي أيضًا بيانات شخصية وفقًا للوائح، ووفقًا للتفسير المتكرر للمجلس الأوروبي لحماية البيانات. الخدمة التي تجمع البيانات الوصفية من الاتصالات المهنية للمستخدم تعالج البيانات الشخصية لعملاء ذلك المستخدم، دون علمهم أو إعطائهم أي موافقة على مثل هذه المعالجة.

إن نمط التفكير الشائع – "أنا أستخدم التطبيق للكتابة فقط؛ التطبيق ليس مزود بيانات لعميلي" – خاطئ قانونيًا. إذا مرت بيانات العميل عبر البنية التحتية لطرف ثالث، فإن هذا الطرف الثالث يعالج تلك البيانات. وإذا كان يعالجها، فيجب أن يكون هناك أساس قانوني، وعقد معالجة بيانات وضمانات كافية.

من المسؤول

مسألة من يتحمل المسؤولية القانونية ليست أكاديمية. تفرق GDPR بين *المتحكم في البيانات* (الذي يقرر البيانات التي تتم معالجتها ولأي غرض) وبين *المعالج* (الذي يقوم بذلك ماديًا نيابة عن المتحكم). المهني الذي يرسل مستندات العملاء هو المتحكم. مزود تطبيق المراسلة هو في كثير من الحالات المعالج الفعلي. بدون عقد معالجة – وبدون معظم البنود التي يجب أن يتضمنها مثل هذا العقد – لم يوفِ المتحكم بالتزامه.

التفسير المتساهل يقول: "معظم المهنيين لا يعرفون ذلك". التفسير الصارم يقول: "الجهل بالقانون لا يعفي من المسؤولية". وعادة ما يكون تفسير أي محامٍ متخصص في حماية البيانات يتم استشارته بهذا الخصوص هو التفسير الصارم.

لمن يهم هذا بشكل ملموس

لكل مهني أو شركة تتعامل، ولو من حين لآخر، مع معلومات شخصية لأطراف ثالثة:

- المحامون الذين يتلقون وثائق العملاء (عقود، دعاوى، إقرارات، تقارير ممتلكات).
- الأطباء وغيرهم من المهنيين الصحيين الذين يشاركون البيانات الصحية – والتي تعتبر *فئات خاصة* بموجب المادة 9 من GDPR مع نظام حماية معزز –.
- المستشارون الضريبيون والمديرون الإداريون الذين يتعاملون مع بيانات الهوية والبيانات الضريبية والمصرفية.
- أقسام الموارد البشرية التي تدير وثائق العمل والوثائق الشخصية للموظفين.
- المندوبون التجاريون الذين يتلقون بيانات الاتصال وغالبًا معلومات تجارية حساسة من العملاء المحتملين والحاليين.

في جميع الحالات، المعلومات محمية بموجب GDPR. في جميع الحالات، في الممارسة المعتادة، تتدفق هذه المعلومات عبر قنوات لا تسمح ولايتها القضائية بإعلانها "معادلة في جوهرها" للإطار الأوروبي دون ضمانات إضافية. ليس عن سوء نية. بل بدافع العادة. وبسبب بنية تحتية تكنولوجية وضعت الراحة قبل الامتثال لمدة خمسة عشر عامًا.

حجة "الجميع يفعل ذلك"

من الحكمة توقع الاعتراض الأكثر شيوعًا: "إذا كان الجميع يفعل ذلك، فلا يمكن أن يكون مشكلة حقيقية". إنها حجة مفهومة تمامًا وليس لها أي قوة قانونية. حقيقة أن ممارسة ما واسعة الانتشار لا تجعلها متوافقة مع اللائحة. قامت سلطات حماية البيانات (مثل الوكالة الإسبانية لحماية البيانات AEPD) بفرض عقوبات في السنوات الأخيرة على العديد من الشركات بالضبط بسبب طرق استخدام المراسلة التي كانت تبدو غير ضارة حتى لحظة التفتيش.

الواقع التشغيلي الحالي هو أن المخاطر من حيث الاحتمالية منخفضة – من النادر جدًا أن يقوم تفتيش من السلطة بالتدقيق في أدوات المراسلة المحددة لمكتب متوسط الحجم – ولكنها عالية من حيث التأثير إذا تحققت. إنه خطر يتحمله معظم الناس دون أن يعرفوا أنهم يتحملونه. أي دون تقييم ما إذا كانت الأداة المستخدمة تتماشى مع المسؤولية القانونية للمتحكم في البيانات.

الآثار الرقمية ذات أثر رجعي

هناك حجة ثانية، شبه متناظرة مع السابقة، تستحق التوقع: *"لو كانت هذه مشكلة خطيرة، لكانت الإدارة قد بدأت بالفعل في مراقبتها"*. الواقع الحالي الملحوظ يعطيها حقًا سطحيًا. عمليات التفتيش بسبب الاستخدام غير السليم للمراسلة في الشركات الصغيرة وخاصة لدى العاملين لحسابهم الخاص تكاد تكون معدومة اليوم – ليس لأن السلوك مسموح به، ولكن لأن الإدارة في معظم دول الاتحاد الأوروبي تفتقر إلى الموارد البشرية اللازمة لتدقيق ملايين الكيانات الملزمة.

هذا ما توحي به الممارسة الملحوظة اليوم. لكن ليس هذا ما يوحي به العقد القادم. يلتقي عاملان لتغيير التوازن في فترات زمنية قصيرة نسبيًا.

أولاً: الآثار الرقمية ذات أثر رجعي. كل رسالة يتم إرسالها عبر تطبيق بخادم مركزي تظل مسجلة – على الأقل في البيانات الوصفية – في بنية تحتية تستمر. ما تم إرساله قبل ستة أشهر لا يزال قابلًا للتدقيق تقنيًا اليوم. ما يتم إرساله اليوم سيكون قابلًا للتدقيق في غضون خمس سنوات. غياب التفتيش في الحاضر ليس ضمانًا لغياب التفتيش في المستقبل. إنه تأجيل للتقييم، وليس إعفاء منه.

ثانيًا: ستنمو قدرة التفتيش الإداري بشكل متسارع. إن إدخال أدوات الذكاء الاصطناعي في عمليات المراقبة يلغي عنق الزجاجة البشري الذي حمى حتى الآن – فعليًا، وليس قانونيًا – الشركات الصغيرة والعاملين لحسابهم الخاص. نظام قادر على المقارنة المرجعية لكميات هائلة من البيانات الوصفية، والإقرارات الضريبية، والسجلات التجارية، والتزامات الإخطار بانتهاكات الأمن لا يحتاج إلى مفتشين: يحتاج إلى وصول. والوصول عبر طلبات للمزودين ذوي الوجود القانوني في الاتحاد الأوروبي ضمن الإطار المعياري الحالي هو أمر ممكن تمامًا.

يضاف إلى ذلك عامل أقل تقنية ولكنه حاسم بنفس القدر: الدول الأوروبية تمر بعملية مديونية متزايدة باستمرار وتحتاج، دون استثناء تقريبًا، إلى توسيع قاعدتها الضريبية. العقوبة الإدارية الناجمة عن عدم الالتزام بـ GDPR هي، بمصطلحات مالية بحتة، مصدر دخل متنامٍ ومريح سياسيًا. هذا ليس افتراضًا: إنه اتجاه ملحوظ في التقارير السنوية لسلطات حماية البيانات الأوروبية، حيث يرتفع الحجم الإجمالي للعقوبات لعدة سنوات مالية متتالية.

الاستنتاج التشغيلي للمسؤول عن البيانات ليس تهويليًا بل رصين: **القرار بشأن كيفية إدارة التواصل مع العملاء اليوم يتم تقييمه مقابل قدرة التفتيش في السنة التي يأتي فيها التفتيش، وليس مقابل القدرة الحالية.** وتلك القدرة ستكون، في غضون فترة زمنية معقولة، مختلفة تمامًا عما هي عليه اليوم. من يبدأ في فعل الأشياء بشكل صحيح اليوم لن يكون في وضع سليم فقط من اليوم فصاعدًا: الأثر الناتج من هذه اللحظة سيكون متوافقًا مع القاعدة، وهذا يحمي بأثر رجعي الفترة القادمة. من يستمر كما كان من قبل سيراكم أثرًا قابلًا للتدقيق سيتم تقييم امتثاله وفقًا لمعايير – وموارد – السنوات القادمة.

ما الذي يتغير مع بنية مختلفة

توجد بدائل تقنية لا يتم فيها تخزين البيانات في البنية التحتية لأطراف ثالثة، بل تنتقل مباشرة من جهاز المرسل إلى جهاز المستلم. في هذه البنية، لا يعتمد الامتثال لـ GDPR فيما يتعلق بالنقل الدولي على البنود التعاقدية القياسية، ولا على حسن نية المزود، ولا على عمليات التدقيق المستقبلية. بل يعتمد على *عدم وجود نقل*. وما لا وجود له لا يمكن انتهاكه.

هذا ليس حلاً حصريًا ولا هو الحل الوحيد الممكن. ولكنه مختلف هيكليًا، ويتوقف الامتثال المعياري عن كونه ملحقًا إجرائيًا ويصبح نتيجة مباشرة للتصميم. بالنسبة للمهني الذي يأخذ مسؤوليته كمسؤول عن البيانات على محمل الجد، فإن هذا الفرق يحدث فرقًا.

العدد القادم من Cuadernos سيحلل بالتفصيل حكم Schrems II وآثاره العملية على الشركات الصغيرة والمتوسطة التي تعتمد على الخدمات السحابية الأمريكية، بعد خمس سنوات من نشره.

ملاحظة هيئة التحرير: عندما تذكر هذه الـ Cuadernos شركات أو منتجات، فليس ذلك للاتهام. فالذين يبنونها يقومون بأعمال يستخدمها الملايين ويقدرونها. ما نشير إليه هو هيكلي — النموذج، وليس العلامة التجارية. تظهر العلامات التجارية كأمثلة لأنها التي يتعرف عليها القارئ.

المصادر والإطار المعياري

- اللائحة (الاتحاد الأوروبي) 2016/679 (GDPR)، وبشكل خاص الفصل الخامس المتعلق بعمليات النقل الدولي.
- محكمة العدل الأوروبية، 16 يوليو 2020، C-311/18 ("Schrems II").
- EDPB – توصيات 01/2020 بشأن التدابير التي تكمل أدوات النقل.
- سلطات حماية البيانات – التقارير السنوية مع حالات العقوبات بسبب الاستخدام غير السليم للمراسلة الفورية في البيئات المهنية.

← السابقالسر المهني في العصر الرقميالتالي → عندما لا يوجد أحد في المنتصف

قراءات حديثة

- تحليل · ١٨ مايو ٢٠٢٦ الخصوصية الحقيقية مقابل الظاهرية: الأسئلة التي ينبغي طرحها
- تحليل · ١٨ مايو ٢٠٢٦ الاستضافة الذاتية كممارسة مهنية
- مفهوم · ١٨ مايو ٢٠٢٦ الـ 24 كلمة: ما هي الهوية التشفيرية

خذ هذا المقال معك أينما احتجت إليه.

↓ ماركداون ↓ نص عادي ↓ PDF

سيتم تنزيل الملف على جهازك. من هناك يمكنك حفظه، أو استيراده إلى Solo2 أو مشاركته أينما تريد. Cuadernos لا تقرر الوجهة نيابة عنك.

ختم شمعي · SHA-256 cc801db7bf25671c270d1196e684cd5d635751d0e721e003bd96babb025d1323

Cuadernos Lacre · منشور لشركة Menzuri Gestión S.L. ·
بقلم R.Eugenio · تحرير فريق Solo2.

هذا الموقع لا يستخدم ملفات تعريف الارتباط ولا يحمل موارد من جهات خارجية. يستخدم عداد زيارات مجهول مستضاف ذاتيًا (Umami، على خادمنا الأوروبي) والحد الأدنى من جافا سكريبت اللازم لعنصري التحكم في الرأس: المظهر الفاتح أو الداكن، ومحدد اللغة. بدون أدوات تتبع، بدون بروفايل، بدون مشاركة بيانات. إذا كنت تريد متابعتنا: RSS.