GDPR و پیام‌رسانی حرفه‌ای: چرا اکثر مردم ندانسته قوانین را نقض می‌کنند

تقریباً هر دفتر، کلینیک یا شرکت مشاوره‌ای اسناد مشتریان را از طریق اپلیکیشن‌هایی ارسال می‌کند که سرور آن‌ها در خارج از منطقه اقتصادی اروپا قرار دارد. بدون نیت سوء، اما در بسیاری از موارد با نقض مقررات و بدون اینکه کسی به آن‌ها هشدار داده باشد.

سندی که دورتر از آنچه فکر می‌کنید سفر می‌کند

یک موقعیت روزمره: یک مشاور مالیاتی از طریق پیام‌رسان سندی حاوی داده‌های مشتری دریافت می‌کند. یک فروشنده از طریق چت پیشنهادی را برای همکارش می‌فرستد. یک پزشک به همان روش گزارشی بالینی را با یک همکار به اشتراک می‌گذارد. هیچ‌کس دو بار فکر نمی‌کند. این عادی است. راحت است. این کاری است که هر روز در هر دفتر در هر شهر اروپایی انجام می‌شود.

اما این سند، در بسیاری از موارد، همین الان به سروری در ایالات متحده سفر کرده است. ذخیره شده است – هرچند موقتی، هرچند "رمزنگاری شده در حالت استراحت" – در ابری که نه متخصص و نه مشتری او کنترلی بر آن ندارند. از سیستم‌هایی عبور کرده است که می‌توانند از نظر فنی متادیتاهای مرتبط با محتوا را ایندکس کنند. و مقررات عمومی حفاظت از داده‌های اروپا در این باره حرف‌های کاملاً روشنی برای گفتن دارد.

آنچه استاندارد ایجاب می‌کند

GDPR – و به تبع آن آرای وحدت رویه دیوان عدالت اتحادیه اروپا (به ویژه حکم Schrems II, C-311/18، در سال ۲۰۲۰) – تعیین می‌کند که داده‌های شخصی شهروندان اروپایی باید به طور مناسب محافظت شوند. اگر این داده‌ها از منطقه اقتصادی اروپا خارج شوند، مسئول داده‌ها باید تضمین کند که دریافت‌کننده سطح حفاظتی "اساساً معادل" سطح اروپایی را ارائه می‌دهد. در عمل، این بدان معناست که ارسال داده‌های مشتریان از طریق سرویس‌هایی که سرورهای آن‌ها تحت صلاحیت قضایی ایالات متحده است، بدون انجام ارزیابی تأثیر و بدون اجرای تضمین‌های تکمیلی – بندهای قراردادی استاندارد، اقدامات فنی اضافی مانند رمزنگاری قابل تأیید و غیره – می‌تواند به معنای نقض مقررات باشد. حتی اگر تا به حال کسی چیزی نگفته باشد.

و موضوع فقط محتوای پیام‌ها نیست. متادیتاها – چه کسی چه چیزی را برای چه کسی می‌فرستد، چه زمانی، چند وقت یک‌بار، از کجا – نیز طبق مقررات و بر اساس تفسیرهای مکرر هیئت حفاظت از داده‌های اروپا، داده شخصی محسوب می‌شوند. سرویسی که متادیتاها را از ارتباطات حرفه‌ای یک کاربر جمع‌آوری می‌کند، داده‌های شخصی مشتریان آن کاربر را بدون اطلاع آن‌ها یا دادن هرگونه رضایتی برای چنین پردازشی، پردازش می‌کند.

طرح فکری رایج – "من فقط از اپلیکیشن برای نوشتن استفاده می‌کنم؛ اپلیکیشن تامین‌کننده داده‌های مشتری من نیست" – از نظر قانونی غلط است. اگر داده‌های مشتری از زیرساخت یک شخص ثالث عبور کنند، آن شخص ثالث در حال پردازش آن داده‌ها است. و اگر در حال پردازش آن‌هاست، باید مبنای قانونی، قرارداد پردازش داده‌ها و تضمین‌های مناسب وجود داشته باشد.

چه کسی مسئول است

مسئله اینکه چه کسی مسئولیت قانونی را بر عهده دارد، آکادمیک نیست. GDPR بین *مسئول داده* (کسی که تصمیم می‌گیرد چه داده‌هایی برای چه هدفی پردازش شوند) و *پردازشگر* (کسی که این کار را به صورت مادی از طرف مسئول انجام می‌دهد) تفاوت قائل می‌شود. متخصصی که اسناد مشتریان را ارسال می‌کند، مسئول داده است. ارائه‌دهنده اپلیکیشن پیام‌رسان در بسیاری از موارد در واقع پردازشگر است. بدون قرارداد پردازش – و بدون اکثر بندهایی که چنین قراردادی باید شامل شود – مسئول داده به تعهد خود عمل نکرده است.

تفسیر ملایم می‌گوید: "اکثر متخصصان این را نمی‌دانند". تفسیر سخت‌گیرانه می‌گوید: "جهل به قانون رافع مسئولیت نیست". و تفسیر هر وکیل متخصص در حفاظت از داده‌ها که در این باره مورد مشورت قرار گیرد، معمولاً تفسیر سخت‌گیرانه است.

این موضوع به طور مشخص برای چه کسانی اهمیت دارد

برای هر متخصص یا شرکتی که حتی به صورت موردی، با اطلاعات شخصی اشخاص ثالث سر و کار دارد:

- وکلایی که اسناد مشتریان را دریافت می‌کنند (قراردادها، دادخواست‌ها، اظهارنامه‌ها، گزارش‌های اموال).
- پزشکان و سایر متخصصان سلامت که داده‌های بهداشتی را به اشتراک می‌گذارند – که طبق ماده ۹ GDPR به عنوان *دسته بندی‌های خاص* با رژیم حفاظتی تقویت شده در نظر گرفته می‌شوند –.
- مشاوران مالیاتی و مدیران اداری که با داده‌های هویتی، مالیاتی و بانکی کار می‌کنند.
- بخش‌های منابع انسانی که اسناد کاری و شخصی کارکنان را مدیریت می‌کنند.
- نمایندگان تجاری که اطلاعات تماس و اغلب اطلاعات تجاری حساس را از مشتریان بالقوه و مشتریان فعلی دریافت می‌کنند.

در تمام موارد، اطلاعات توسط GDPR محافظت می‌شوند. در تمام موارد، در ممارست معمول، این اطلاعات از طریق کانال‌هایی جریان می‌یابند که حوزه قضایی آن‌ها اجازه نمی‌دهد بدون تضمین‌های اضافی، به عنوان "اساساً معادل" چارچوب اروپایی اعلام شوند. نه از روی نیت بد. از روی عادت. و به دلیل زیرساخت تکنولوژیکی که به مدت پانزده سال راحتی را بر انطباق ترجیح داده است.

حجت «همه این کار را می‌کنند»

منطقی است که رایج‌ترین اعتراض را پیش‌بینی کنیم: "اگر همه این کار را می‌کنند، نمی‌تواند یک مشکل واقعی باشد". این یک استدلال کاملاً قابل درک است و از نظر قانونی هیچ قدرتی ندارد. این واقعیت که یک ممارست گسترده است، آن را با مقررات منطبق نمی‌کند. مقامات حفاظت از داده‌ها در سال‌های اخیر چندین شرکت را دقیقاً به دلیل روش‌های استفاده از پیام‌رسانی که تا لحظه بازرسی بی‌ضرر به نظر می‌رسیدند، جریمه کرده‌اند.

واقعیت عملیاتی فعلی این است که ریسک از نظر احتمال پایین است – بسیار نادر است که بازرسی مقامات، ابزارهای پیام‌رسانی خاص یک دفتر متوسط را ممیزی کند – اما از نظر تأثیر در صورت وقوع، بالاست. این ریسکی است که اکثر مردم بدون اینکه بدانند در حال پذیرش آن هستند، می‌پذیرند. یعنی بدون ارزیابی اینکه آیا ابزار مورد استفاده با مسئولیت قانونی مسئول داده‌ها همسو است یا خیر.

آثار دیجیتال دارای اثر رجعی هستند

حجت دومی وجود دارد، تقریباً متقارن با قبلی، که ارزش پیش‌بینی دارد: «*اگر این یک مشکل جدی بود، دولت قبلاً نظارت بر آن را شروع کرده بود*». واقعیت ملحوظ فعلی به آن حقی سطحی می‌دهد. بازرسی‌ها به دلیل استفاده نامناسب از پیام‌رسانی در شرکت‌های کوچک و به ویژه در میان مشاغل آزاد امروزه تقریباً وجود ندارند – نه به این دلیل که رفتار مجاز باشد، بلکه به این دلیل که دولت در اکثر کشورهای اتحادیه اروپا فاقد منابع انسانی لازم برای ممیزی میلیون‌ها نهاد متعهد است.

این چیزی است که ممارست ملحوظ امروز القا می‌کند. اما این چیزی نیست که دهه آینده القا می‌کند. دو عامل برای تغییر تعادل در بازه‌های زمانی نسبتاً کوتاه همگرا می‌شوند.

اولاً: آثار دیجیتال دارای اثر رجعی هستند. هر پیامی که از طریق یک اپلیکیشن با سرور مرکزی ارسال می‌شود، حداقل در متادیتاها، در زیرساختی که تداوم دارد ثبت می‌ماند. آنچه شش ماه پیش ارسال شده است، امروزه هنوز از نظر فنی قابل ممیزی است. آنچه امروز ارسال می‌شود، تا پنج سال دیگر قابل ممیزی خواهد بود. نبود بازرسی در حال حاضر تضمینی برای نبود بازرسی در آینده نیست. این یک تأخیر در ارزیابی است، نه معافیت از آن.

ثانیاً: ظرفیت بازرسی دولتی به طور متسارع رشد خواهد کرد. ورود ابزارهای هوش مصنوعی در فرآیندهای نظارتی، گلوگاه انسانی را که تا کنون – در عمل و نه در قانون – از شرکت‌های کوچک و مشاغل آزاد محافظت می‌کرد، از بین می‌برد. سیستمی که قادر به مقایسه مرجع مقادیر عظیمی از متادیتاها، اظهارنامه‌های مالیاتی، دفاتر تجاری و تعهدات اطلاع‌رسانی نقض امنیت باشد، نیازی به بازرس ندارد: نیاز به دسترسی دارد. و دسترسی از طریق درخواست از تامین‌کنندگانی با حضور قانونی در اتحادیه اروپا در چارچوب هنجاری فعلی کاملاً امکان‌پذیر است.

به این مورد یک عامل کمتر فنی اما به همان اندازه تعیین‌کننده اضافه می‌شود: کشورهای اروپایی در فرآیند بدهی فزاینده مداوم هستند و تقریباً بدون استثنا باید پایه مالیاتی خود را گسترش دهند. جریمه اداری ناشی از عدم پایبندی به GDPR، از نظر مالی محض، یک منبع درآمد در حال رشد و از نظر سیاسی راحت است. این یک فرض نیست: این یک روند ملحوظ در گزارش‌های سالانه مقامات حفاظت از داده‌های اروپایی است، جایی که حجم کل جریمه‌ها برای چندین سال مالی متوالی در حال افزایش است.

نتیجه‌گیری عملیاتی برای مسئول داده‌ها هشداردهنده نیست بلکه واقع‌بینانه است: **تصمیم درباره نحوه مدیریت ارتباط با مشتریان در امروز، در مقابل ظرفیت بازرسی سالی که بازرسی در آن انجام می‌شود سنجیده می‌شود، نه در مقابل ظرفیت فعلی.** و آن ظرفیت در یک بازه زمانی معقول، تفاوت اساسی با امروز خواهد داشت. کسی که از امروز شروع به انجام درست کارها می‌کند، فقط از امروز به بعد در وضعیت سالم نخواهد بود: اثری که از این لحظه به بعد ایجاد می‌شود مطابق با قاعده خواهد بود و این از دوره پیش رو به صورت رجعی محافظت می‌کند. کسی که مانند قبل ادامه دهد، اثری قابل ممیزی را انباشته خواهد کرد که انطباق آن بر اساس استانداردهای – و منابع – سال‌های آینده ارزیابی خواهد شد.

چه چیزی با یک معماری متفاوت تغییر می‌کند

جایگزین‌های فنی وجود دارند که در آن‌ها داده‌ها در زیرساخت اشخاص ثالث ذخیره نمی‌شوند، بلکه مستقیماً از دستگاه فرستنده به دستگاه گیرنده سفر می‌کنند. در این معماری، انطباق با GDPR در رابطه با انتقال بین‌المللی به بندهای قراردادی استاندارد، نه به حسن نیت تامین‌کننده و نه به ممیزی‌های آینده بستگی ندارد. بلکه به این بستگی دارد که *انتقالی وجود ندارد*. و چیزی که وجود ندارد را نمی‌توان نقض کرد.

این تنها راهکار نیست و تنها راهکار ممکن هم نیست. اما از نظر ساختاری متفاوت است و انطباق هنجاری دیگر یک ضمیمه رویه‌ای نیست بلکه به نتیجه مستقیم طراحی تبدیل می‌شود. برای متخصصی که مسئولیت خود را به عنوان مسئول داده جدی می‌گیرد، این تفاوت اهمیت دارد.

شماره آینده Cuadernos حکم Schrems II و پیامدهای عملی آن را برای شرکت‌های کوچک و متوسط وابسته به خدمات ابری ایالات متحده، پنج سال پس از انتشار آن، به تفصیل تحلیل خواهد کرد.

منابع و چارچوب هنجاری

- لائحه (اتحادیه اروپا) 2016/679 (GDPR)، به ویژه فصل پنجم مربوط به عملیات انتقال بین‌المللی.
- دیوان عدالت اروپا ۱۶ ،("Schrems II") C-311/18 ژوئیه ۲۰۲۰.
- EDPB – توصیه 01/2020 درباره اقداماتی که ابزارهای انتقال را تکمیل می‌کنند.
- مقامات حفاظت از داده‌ها – گزارش‌های سالانه با موارد جریمه به دلیل استفاده نامناسب از پیام‌رسانی فوری در محیط‌های حرفه‌ای.

← السابقرازداری حرفه‌ای در عصر دیجیتالالتالي → وقتی هیچ‌کس در میان نیست

قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ مارک‌داون ↓ متن ساده ↓ PDF

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعي · SHA-256 90cb55531d8509d66d33fb0a45223504675c7fbc7a3d106a9f9d364575261bbe

Cuadernos Lacre · نشريّة من Menzuri Gestión S.L. ·
كتبها R.Eugenio · حرّرها فريق Solo2.

این وب‌سایت از کوکی استفاده نمی‌کند و منابع شخص ثالث را بارگذاری نمی‌کند. این سایت از یک شمارنده بازدید ناشناس خود-میزبان (Umami، روی سرور اروپایی ما) و حداقل جاوا اسکریپت لازم برای تنظیم تم روشن/تاریک شما استفاده می‌کند. بدون ردیاب، بدون پروفایل‌سازی، بدون اشتراک‌گذاری داده‌ها. اگر می‌خواهید ما را دنبال کنید: RSS.