Phân tích · 16 tháng 5, 2026

← Trước·Tiếp theo →

GDPR và tin nhắn chuyên nghiệp: tại sao hầu hết đang vi phạm mà không hề hay biết

Hầu hết mọi văn phòng, phòng khám hoặc công ty tư vấn đều gửi tài liệu khách hàng qua các ứng dụng nhắn tin có máy chủ đặt ngoài Khu vực Kinh tế Châu Âu. Không có ác ý, nhưng trong nhiều trường hợp đang vi phạm quy định mà không ai cảnh báo họ.

Tài liệu đi xa hơn bạn nghĩ

Một tình huống hàng ngày: một chuyên gia tư vấn thuế nhận được qua tin nhắn một tài liệu chứa dữ liệu khách hàng. Một nhân viên bán hàng chuyển tiếp qua chat một đề nghị cho đồng nghiệp. Một bác sĩ chia sẻ cùng cách đó một báo cáo lâm sàng với cộng sự. Không ai nghĩ ngợi lần thứ hai. Điều đó là bình thường. Tiện lợi. Đó là những gì được thực hiện hàng ngày tại mọi văn phòng ở mọi thành phố ở Châu Âu.

Nhưng tài liệu này, trong nhiều trường hợp, vừa mới di chuyển đến một máy chủ tại Hoa Kỳ. Nó đã được lưu trữ – dù chỉ là tạm thời, dù là "mã hóa tại chỗ" – trong một đám mây mà cả chuyên gia lẫn khách hàng đều không kiểm soát. Nó đã đi qua các hệ thống có thể lập chỉ mục các siêu dữ liệu liên quan đến nội dung về mặt kỹ thuật. Và Quy định chung về bảo vệ dữ liệu của Châu Âu có những điều khá rõ ràng để nói về điều này.

Tiêu chuẩn yêu cầu gì

GDPR – và theo đó là án lệ của Tòa án Công lý Liên minh Châu Âu (đặc biệt là phán quyết Schrems II, C-311/18, năm 2020) – xác định rằng dữ liệu cá nhân của công dân Châu Âu phải được bảo vệ thích đáng. Nếu những dữ liệu này rời khỏi Khu vực Kinh tế Châu Âu, bên kiểm soát dữ liệu phải đảm bảo rằng bên nhận cung cấp mức độ bảo vệ "tương đương về bản chất" với mức độ của Châu Âu. Trong thực tế, điều này có nghĩa là việc gửi dữ liệu khách hàng thông qua các dịch vụ có máy chủ thuộc quyền tài phán của Hoa Kỳ, mà không thực hiện đánh giá tác động và không triển khai các biện pháp đảm bảo bổ sung – các điều khoản hợp đồng tiêu chuẩn, các biện pháp kỹ thuật bổ sung như mã hóa có thể xác minh, v.v. – có thể cấu thành hành vi vi phạm quy định. Ngay cả khi cho đến nay chưa ai nói gì.

Và vấn đề không chỉ nằm ở nội dung tin nhắn. Siêu dữ liệu – ai gửi gì cho ai, khi nào, tần suất ra sao, từ đâu – cũng là dữ liệu cá nhân theo các quy định, theo cách giải thích lặp đi lặp lại của Ban Bảo vệ Dữ liệu Châu Âu. Một dịch vụ thu thập siêu dữ liệu từ các liên lạc chuyên môn của người dùng đang xử lý dữ liệu cá nhân của các khách hàng của người dùng đó, mà họ không hề biết hoặc đưa ra bất kỳ sự đồng ý nào cho việc xử lý như vậy.

Mô hình tư duy thông thường – "tôi chỉ dùng ứng dụng để viết; ứng dụng không phải là nhà cung cấp dữ liệu cho khách hàng của tôi" – là sai lầm về mặt pháp lý. Nếu dữ liệu của khách hàng đi qua cơ sở hạ tầng của bên thứ ba, thì bên thứ ba đó đang xử lý những dữ liệu đó. Và nếu họ xử lý chúng, thì phải có cơ sở pháp lý, hợp đồng xử lý dữ liệu và các biện pháp đảm bảo thích hợp.

Ai là người chịu trách nhiệm

Câu hỏi về việc ai chịu trách nhiệm pháp lý không phải là câu hỏi lý thuyết. GDPR phân biệt giữa *bên kiểm soát dữ liệu* (người quyết định dữ liệu nào được xử lý và vì mục đích gì) và *bên xử lý dữ liệu* (người thực hiện việc đó về mặt vật chất thay mặt cho bên kiểm soát). Chuyên gia gửi tài liệu khách hàng là bên kiểm soát dữ liệu. Nhà cung cấp ứng dụng nhắn tin trong nhiều trường hợp là bên xử lý dữ liệu trên thực tế. Nếu không có hợp đồng xử lý – và thiếu hầu hết các điều khoản mà một hợp đồng như vậy phải có – bên kiểm soát đã không thực hiện đúng nghĩa vụ của mình.

Cách giải thích nhẹ nhàng là: "hầu hết các chuyên gia không biết điều này". Cách giải thích cứng rắn là: "thiếu hiểu biết về luật pháp không phải là lý do bào chữa". Và cách giải thích của bất kỳ luật sư chuyên về bảo vệ dữ liệu nào được tham vấn về vấn đề này thường là cách giải thích cứng rắn.

Điều này quan trọng cụ thể với ai

Dành cho mọi chuyên gia hoặc công ty làm việc, dù chỉ thỉnh thoảng, với thông tin cá nhân của bên thứ ba:

- Luật sư nhận hồ sơ khách hàng (hợp đồng, đơn kiện, tờ khai, báo cáo tài sản).
- Bác sĩ và các chuyên gia y tế khác chia sẻ dữ liệu sức khỏe – vốn được coi theo Điều 9 GDPR là *danh mục đặc biệt* với chế độ bảo vệ tăng cường –.
- Chuyên gia tư vấn thuế và quản lý hành chính làm việc với dữ liệu nhận dạng, thuế và ngân hàng.
- Bộ phận nhân sự quản lý hồ sơ công việc và cá nhân của nhân viên.
- Đại diện thương mại nhận chi tiết liên lạc và thường là thông tin kinh doanh nhạy cảm từ các khách hàng tiềm năng và khách hàng hiện tại.

Trong mọi trường hợp, thông tin đều được GDPR bảo vệ. Trong mọi trường hợp, theo thông lệ thông thường, thông tin này chảy qua các kênh mà quyền tài phán của chúng không cho phép tuyên bố chúng là "tương đương về bản chất" với khung quy định của Châu Âu nếu không có các đảm bảo bổ sung. Không phải vì ác ý. Vì thói quen. Và vì cơ sở hạ tầng công nghệ trong mười lăm năm qua đã đặt sự tiện lợi lên trên sự tuân thủ.

Lập luận "ai cũng làm thế"

Cần lường trước sự phản đối phổ biến nhất: "nếu ai cũng làm như vậy, thì đó không thể là một vấn đề thực sự". Đây là một lập luận hoàn toàn có thể hiểu được về mặt cảm tính nhưng về mặt pháp lý thì không có giá trị gì. Việc một thói quen phổ biến không làm cho nó trở nên tuân thủ quy định. Các cơ quan bảo vệ dữ liệu trong những năm gần đây đã xử phạt nhiều công ty chính vì các cách thức sử dụng tin nhắn vốn có vẻ vô hại cho đến thời điểm kiểm tra.

Thực tế vận hành hiện nay là rủi ro về mặt xác suất là thấp – rất hiếm khi một cuộc thanh tra của Cơ quan chức năng tiến hành kiểm tra các công cụ nhắn tin cụ thể của một văn phòng quy mô trung bình – nhưng lại cao về mặt tác động nếu nó xảy ra. Đó là một rủi ro mà hầu hết mọi người đang gánh chịu mà không biết mình đang gánh chịu. Nghĩa là, không đánh giá xem công cụ đang sử dụng có phù hợp với trách nhiệm pháp lý của bên kiểm soát dữ liệu hay không.

Dấu vết kỹ thuật số có tính hồi tố

Có một lập luận thứ hai, gần như đối xứng với lập luận trước đó, đáng để chúng ta dự báo: *"nếu đây là một vấn đề nghiêm trọng, chính quyền hẳn đã bắt đầu kiểm soát nó rồi"*. Thực tế quan sát hiện nay cho thấy lập luận này có vẻ đúng về bề mặt. Các cuộc thanh tra do sử dụng tin nhắn không đúng cách trong các công ty nhỏ và đặc biệt là ở những người hành nghề tự do ngày nay hầu như không tồn tại – không phải vì hành vi đó được phép, mà vì chính quyền ở hầu hết các nước EU thiếu nhân lực cần thiết để kiểm tra hàng triệu đối tượng có nghĩa vụ.

Đó là những gì thực tế quan sát được hôm nay gợi ý. Nhưng đó không phải là những gì thập kỷ tới gợi ý. Hai vectơ đang hội tụ để thay đổi sự cân bằng trong khoảng thời gian tương đối ngắn.

Thứ nhất: dấu vết kỹ thuật số có tính hồi tố. Mọi tin nhắn được gửi qua một ứng dụng có máy chủ trung tâm đều được ghi lại – ít nhất là trong siêu dữ liệu – trong một cơ sở hạ tầng tồn tại lâu dài. Những gì được gửi đi từ sáu tháng trước về mặt kỹ thuật vẫn có thể được kiểm tra vào ngày hôm nay. Những gì được gửi hôm nay vẫn có thể được kiểm tra trong năm năm tới. Việc thiếu thanh tra ở hiện tại không phải là sự đảm bảo cho việc thiếu thanh tra trong tương lai. Đó là sự trì hoãn đánh giá, chứ không phải sự miễn trừ.

Thứ hai: năng lực thanh tra hành chính sẽ tăng tốc mạnh mẽ. Việc đưa các công cụ trí tuệ nhân tạo vào quy trình kiểm soát sẽ loại bỏ nút thắt cổ chai về nhân lực vốn từ trước đến nay đã bảo vệ – trên thực tế chứ không phải về mặt pháp lý – các công ty nhỏ và những người hành nghề tự do. Một hệ thống có khả năng đối chiếu chéo các khối siêu dữ liệu khổng lồ, tờ khai thuế, đăng ký kinh doanh và nghĩa vụ thông báo vi phạm bảo mật sẽ không cần thanh tra viên: nó cần quyền truy cập. Và việc truy cập thông qua các yêu cầu đối với các nhà cung cấp có sự hiện diện pháp lý tại EU trong khung định mức hiện tại là hoàn toàn khả thi.

Thêm vào đó là một yếu tố ít mang tính kỹ thuật hơn nhưng cũng mang tính quyết định không kém: các quốc gia Châu Âu đang trong quá trình nợ nần gia tăng liên tục và họ cần, hầu như không có ngoại lệ, mở rộng cơ sở thuế của mình. Hình phạt hành chính phát sinh từ việc không tuân thủ GDPR, xét về mặt tài khóa thuần túy, là một nguồn thu đang tăng trưởng và thuận tiện về mặt chính trị. Đây không phải là phỏng đoán: đây là một xu hướng có thể quan sát được trong báo cáo thường niên của các cơ quan bảo vệ dữ liệu Châu Âu, nơi tổng số tiền phạt đã tăng trong nhiều năm tài chính liên tiếp.

Kết luận vận hành đối với bên kiểm soát dữ liệu không phải là gây hoang mang mà là sự tỉnh táo: **quyết định về cách quản lý liên lạc với khách hàng ngày hôm nay sẽ được đánh giá dựa trên năng lực thanh tra của năm mà cuộc thanh tra diễn ra, chứ không phải năng lực hiện tại.** Và năng lực đó, trong một khoảng thời gian hợp lý, sẽ khác biệt đáng kể so với ngày nay. Ai bắt đầu làm đúng từ hôm nay sẽ không chỉ ổn kể từ hôm nay: dấu vết được tạo ra từ thời điểm này trở đi sẽ tuân thủ tiêu chuẩn, và điều đó bảo vệ mang tính hồi tố cho giai đoạn sắp tới. Ai tiếp tục như trước đây sẽ tích tụ một dấu vết có thể bị thanh tra mà tính tuân thủ của nó sẽ được đánh giá theo các tiêu chuẩn – và nguồn lực – của những năm tới.

Điều gì thay đổi với một kiến trúc khác

Có những giải pháp kỹ thuật thay thế mà dữ liệu không được lưu trữ trong cơ sở hạ tầng của bên thứ ba, thay vào đó chúng di chuyển trực tiếp từ thiết bị của người gửi đến người nhận. Trong kiến trúc này, việc tuân thủ GDPR liên quan đến chuyển giao quốc tế không phụ thuộc vào các điều khoản hợp đồng tiêu chuẩn, cũng không phụ thuộc vào thiện chí của nhà cung cấp hay các cuộc thanh tra trong tương lai. Nó phụ thuộc vào sự thật rằng *không có sự chuyển giao nào cả*. Và những gì không tồn tại thì không thể bị vi phạm.

Đây không phải là giải pháp duy nhất và cũng không phải là giải pháp khả thi duy nhất. Nhưng nó khác biệt về mặt cấu trúc, và việc tuân thủ định mức không còn là một phụ lục về mặt quy trình mà trở thành hệ quả trực tiếp của thiết kế. Đối với một chuyên gia coi trọng trách nhiệm của mình với tư cách là bên kiểm soát dữ liệu, sự khác biệt đó thực sự quan trọng.

Số tiếp theo của Cuadernos sẽ phân tích chi tiết phán quyết Schrems II và những tác động thực tế của nó đối với các doanh nghiệp vừa và nhỏ phụ thuộc vào các dịch vụ đám mây của Hoa Kỳ, năm năm sau khi phán quyết được công bố.

Nguồn và khung định mức

- Quy định (EU) 2016/679 (GDPR), đặc biệt là Chương V liên quan đến các hoạt động chuyển giao quốc tế.
- CJUE C-311/18 ("Schrems II"), 16 tháng 7, 2020.
- EDPB – Khuyến nghị 01/2020 về các biện pháp bổ sung cho các công cụ chuyển giao.
- Các cơ quan bảo vệ dữ liệu – Báo cáo thường niên với các trường hợp xử phạt do sử dụng tin nhắn tức thời không đúng cách trong môi trường chuyên nghiệp.

← TrướcBí mật nghề nghiệp trong kỷ nguyên sốTiếp theo →Khi không có ai ở giữa

Các bài đọc gần đây

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Tải bài viết này để sử dụng ở bất cứ đâu bạn cần.

↓ Markdown ↓ Văn bản thuần túy ↓ PDF

Tệp sẽ được tải xuống thiết bị của bạn. Từ đó, bạn có thể lưu trữ, nhập vào Solo2 hoặc chia sẻ ở bất cứ đâu. Cuadernos không quyết định điểm đến thay cho bạn.

Dấu sáp · SHA-256 b670cbfe20b63f52b8f6124f61e92311149bf7983fe901e3dd060c7839876049

Cuadernos Lacre · Một ấn phẩm của Menzuri Gestión S.L. ·
viết bởi R.Eugenio · được biên tập bởi đội ngũ Solo2.