分析 · 2026年5月16日

← 前へ·次へ →

GDPR とビジネスチャット：なぜ多くの組織が知らずに違反しているのか

ほぼ全ての法律事務所、診療所、コンサルティング会社が、欧州経済領域（EEA）外にサーバーを持つアプリを通じて、顧客の書類を送信しています。悪意はありませんが、多くの場合、誰にも警告されることなく規制に違反しています。

かみ砕いて言うと： 税理士がWhatsAppで書類を送ってきたとします。マドリードにいるあなたのスマホに届きますが、その前にテキサスのサーバーを経由しています。GDPR（欧州一般データ保護規則）はこの点について非常に明確な見解を持っていますが、ほとんどの事務所は気づかないまま何年も違反を続けています。

想像以上に遠くまで旅をする書類

日常的な光景：税理士がメッセージングアプリで顧客データを含む書類を受け取る。営業担当者がチャットで同僚に見積書を転送する。医師が同じ方法で臨床報告書を同僚と共有する。誰も二度と考えません。それが普通であり、便利だからです。欧州のあらゆる都市の、あらゆるオフィスで毎日行われていることです。

しかしこの書類は、多くの場合、たった今アメリカ合衆国のサーバーへと旅をしました。一時的であれ、「保存時の暗号化」であれ、専門家も顧客も管理していないクラウドに保存されました。内容に関連するメタデータを技術的にインデックス化できるシステムを通過したのです。そして、欧州一般データ保護規則はこの点について、極めて明確な見解を持っています。

規範が求めるもの

GDPR、およびそれに付随する欧州連合司法裁判所の判例（特に2020年の Schrems II 判決、C-311/18）は、欧州市民の個人データが適切に保護されなければならないと定めています。もしデータが EEA を離れる場合、データ管理者は受信側が欧州と「本質的に同等」の保護レベルを提供することを保証しなければなりません。実際問題として、影響評価を行わず、補完的な保証（標準契約条項、検証可能な暗号化などの追加の技術的措置など）を実装せずに、サーバーが米国司法管轄下にあるサービスを通じて顧客データを送信することは、規制違反となる可能性があります。たとえ今まで誰も何も言わなかったとしても、です。

そして、問題はメッセージの内容だけではありません。メタデータ（誰が誰に何を、いつ、どのくらいの頻度で、どこから送ったか）も、規制により、また欧州データ保護会議（EDPB）の繰り返される解釈により、個人データに該当します。ユーザーの業務通信からメタデータを収集するサービスは、そのユーザーの顧客の個人データを、彼らが知ることなく、またそのような処理に同意することなく処理していることになります。

「アプリは書くためだけに使っている。アプリは顧客データの提供者ではない」という一般的な思考パターンは、法的に誤りです。顧客のデータが第三者のインフラを通過する場合、その第三者はデータを処理していることになります。そして処理を行う以上、法的根拠、データ処理契約、および適切な保証が存在しなければなりません。

誰に責任があるのか

法的責任を誰が負うのかという問いは、学術的なものではありません。GDPR は、*データ管理者*（どのデータを何の目的で処理するかを決定する者）と*データ処理者*（管理者に代わって実質的に処理を行う者）を区別します。顧客の書類を送信する専門家は、データ管理者です。メッセージングアプリの提供者は、多くの場合、実質的なデータ処理者です。処理契約を締結せず、またそのような契約に含まれるべき条項の多くを欠いたままでは、管理者は義務を果たしたことになりません。

善意の解釈では「ほとんどの専門家はこれを知らない」となります。厳格な解釈では「法の不知は免責されない」となります。そして、この件に関して相談を受けたデータ保護専門の弁護士の解釈は、通常、後者の厳格なものです。

具体的に誰にとって重要か

たまにであっても第三者の個人情報を取り扱う、すべての専門家や企業にとって重要です：

- 顧客の書類（契約書、訴状、申告書、資産報告書）を受け取る弁護士。
- 健康データを共有する医師や医療従事者。これらは GDPR 第9条に基づき、強化された保護体制が必要な*特別なカテゴリ*と見なされます。
- 識別情報、税務、銀行データを扱う税理士や行政書士。
- 従業員の就業・個人書類を管理する人事部門。
- 見込み客や既存顧客から連絡先や機密性の高いビジネス情報を受け取る営業担当者。

いかなる場合も情報は GDPR によって保護されます。いかなる場合も、一般的な慣行において、これらの情報は、追加の保証なしには欧州の枠組みと「本質的に同等」であると宣言できない法域のチャネルを流れています。悪意からではなく、慣習からです。そして、15年間にわたりコンプライアンスよりも利便性を優先してきた技術インフラの結果です。

「みんなやっている」という論理

最も一般的な反論を予想しておくべきでしょう。「もし全員がやっているなら、本当の問題であるはずがない」というものです。これは完全に理解できる主張ですが、法的には何の効力もありません。ある慣行が普及しているという事実は、それを規制に準拠させるものではありません。データ保護当局は近年、検査の瞬間まで無害に見えたメッセージングの使用形態に対して、まさにいくつかの企業を処罰しています。

現在の運用の現実は、発生確率という点ではリスクは低い（当局の検査が中規模事務所の特定のメッセージングツールを監査することは非常に稀です）ものの、現実となった場合の影響という点では高いということです。それは、ほとんどの人がリスクを冒していると知らずに冒しているリスクです。つまり、使用しているツールがデータ管理者の法的責任と整合しているかどうかを評価していないのです。

デジタルな足跡は遡及的である

前述のものとほぼ対称的な第二の論理があり、これも予想しておく価値があります：*「もしこれが深刻な問題なら、行政はすでに監視を始めているはずだ」*というものです。現在の観察される現実は、表面上はこれを肯定しています。中小企業、特に個人事業主における不適切なメッセージング利用に対する検査は、今日ではほとんど存在しません。それはその行為が許可されているからではなく、日本や EU の大部分の行政において、数百万の対象者を監査するために必要な人的資源が不足しているからです。

これが今日観察される慣行が示唆していることです。しかし、次の10年が示唆していることは異なります。二つのベクトルが収束し、比較的短期間でバランスを変化させようとしています。

第一に、デジタルな足跡は遡及的（過去に遡る）です。 中央サーバーを持つアプリを通じて送信されたすべてのメッセージは、少なくともメタデータにおいては、存続し続けるインフラに記録されたままになります。6ヶ月前に送信されたものは、技術的には今日でも監査可能です。今日送信されるものは、5年後でも監査可能でしょう。現在の検査の欠如は、将来の検査の欠如を保証するものではありません。それは評価の延期であり、免除ではないのです。

第二に、行政の監査能力は加速的に向上します。 監視プロセスへの人工知能（AI）ツールの導入は、これまで中小企業や個人事業主を（法的ではなく事実上）守ってきた人的なボトルネックを解消します。膨大なメタデータ、納税申告書、商業登記、およびセキュリティ侵害の通知義務をクロスチェックできるシステムに、検査官は必要ありません。必要なのはアクセスです。そして、現在の規範的枠組みの下で EU 内に法的拠点を持つプロバイダーに対する要求を通じたアクセスは、完全に実行可能です。

これに、技術的ではないものの同様に決定的な要因が加わります。欧州諸国は絶え間ない債務増大の過程にあり、ほぼ例外なく課税ベースを拡大する必要があります。GDPR 不履行から生じる行政処分は、純粋に財政的な観点から見れば、成長しており、かつ政治的に好都合な収入源です。これは推測ではありません。欧州のデータ保護当局の年次報告書において、制裁金の総額が数会計年度連続で増加しているという観察可能な傾向です。

データ管理者にとっての運用上の結論は、扇動的なものではなく、冷徹なものです：**今日の顧客との通信をどう管理するかという決定は、現在の検査能力ではなく、実際に検査が行われる年の能力に照らして評価されます。** そしてその能力は、妥当な期間内に、今日とは根本的に異なるものになるでしょう。今日から物事を正しく行い始める人は、今日以降が健全であるだけではありません。この瞬間から生成される足跡が規範に準拠したものとなり、それが遡及的にこれからの期間を保護することになります。これまで通り続ける人は、将来の基準とリソースによって適合性が評価されることになる、監査可能な負の遺産を蓄積し続けることになるのです。

別のアーキテクチャで何が変わるのか

データが第三者のインフラに保存されず、送信者のデバイスから受信者のデバイスへと直接移動する技術的な代替案が存在します。このアーキテクチャでは、国際移転に関する GDPR への準拠は、標準契約条項にも、プロバイダーの善意にも、将来の監査にも依存しません。それは、*「移転が存在しない」*という事実に依存します。存在しないものを違反することはできないのです。

これは唯一の解決策でも、唯一可能な方法でもありません。しかし、構造的に異なっており、規範への準拠は手続き上の付随物ではなく、設計の直接的な結果となります。データ管理者としての責任を真剣に捉える専門家にとって、その違いは大きな意味を持ちます。

次回の Cuadernos では、Schrems II 判決と、米国クラウドサービスに依存する中小企業への実務的な影響について、公開から5年が経過した時点での詳細な分析を行います。

編集後記： この「Cuadernos」で企業名や製品名を挙げているのは、決して非難するためではありません。それらを構築している人々は、何百万人もの人々に利用され愛される素晴らしい仕事をしています。私たちが指摘しているのは構造的な問題であり、ブランドではなくモデルの問題です。読者に馴染みがあるため、例としてブランド名を挙げているに過ぎません。

参考文献および法的枠組み

- GDPR（EU 規則 2016/679）、特に国際移転に関する第5章。
- 欧州司法裁判所 C-311/18（"Schrems II"）、2020年7月16日。
- EDPB – 移転ツールを補完する措置に関する勧告 01/2020。
- 各国のデータ保護当局 – 専門的な環境でのインスタントメッセージの不適切な使用による制裁事例を含む年次報告書。

← 前へデジタル時代における守秘義務次へ →真ん中に誰もいないとき

最近の記事

- 分析 · 2026年5月18日 真のプライバシー vs 表向きのプライバシー：問い直すべきこと
- 分析 · 2026年5月18日 専門的実践としてのセルフホスティング
- コンセプト · 2026年5月18日 24個の単語：暗号学的アイデンティティとは何か

この記事をダウンロードして、必要な場所で活用してください。

↓ Markdown ↓ テキスト形式 ↓ PDF

ファイルはお使いのデバイスにダウンロードされます。そこから保存、Solo2 へのインポート、または任意の場所での共有が可能です。Cuadernos が送信先を決定することはありません。

封蝋 · SHA-256 88598d9439f330cb129170ce519e3f39d430d1b8c7a81721de29718fb4e608af

Cuadernos Lacre · Menzuri Gestión S.L. による刊行物 ·
著者：R.Eugenio · 編集：Solo2 チーム