分析 · 2026年5月16日

← 上一页·下一页 →

GDPR 与专业即时通信：为何大多数人都在不知情中违规

几乎所有的事务所、诊所或咨询公司都在通过服务器位于欧洲经济区以外的应用发送客户文件。他们并无恶意，但在很多情况下，他们在无人警告的情况下违反了条例。

文档传输得比您想象的更远

一个日常情景：税务顾问通过即时通信收到一份包含客户数据的文档。销售人员通过聊天将报价转发给同事。医生以同样的方式与合作伙伴分享临床报告。没有人会多想。这很正常。很方便。这就是欧洲每个城市、每个办公室每天都在发生的事情。

但在许多情况下，这份文档刚刚传输到了美国的一台服务器。它被存储了——哪怕是暂时的，哪怕是“静态加密”的——存储在一个专业人士及其客户都无法控制的云端。它经过了一些在技术上能够对与内容相关的元数据进行索引的系统。对此，欧洲《通用数据保护条例》有非常明确的规定。

规范的要求

GDPR 以及随后欧盟司法法院的判例（特别是 2020 年的 Schrems II 裁决，C-311/18）规定，必须妥善保护欧洲公民的个人数据。如果这些数据离开欧洲经济区，数据控制者必须保证接收方提供与欧洲“实质上等同”的保护水平。在实践中，这意味着如果通过服务器受美国司法管辖的服务发送客户数据，而未进行影响评估且未实施补充保证（标准合同条款、可验证加密等额外技术措施等），则可能构成违反条例。尽管到目前为止还没人说什么。

而且问题不仅在于消息内容。根据规定，以及欧洲数据保护委员会（EDPB）的反复解释，元数据（谁在何时、以何种频率、从何处向谁发送了什么）也属于个人数据。收集用户职业通信元数据的服务是在处理该用户客户的个人数据，而这些客户对此并不知情，也未对这种处理给予任何同意。

常见的思维模式——“我只用应用来写字；该应用不是我客户的数据提供商”——在法律上是错误的。如果客户的数据经过第三方的基础设施，该第三方就在处理这些数据。既然在处理数据，就必须有法律依据、数据处理合同和适当的保证。

谁负责

谁承担法律责任的问题并非学术讨论。GDPR 区分了*数据控制者*（决定处理哪些数据以及出于何种目的）和*数据处理者*（代表控制者进行实质操作的人）。发送客户文件的专业人士是控制者。即时通信应用提供商在许多情况下实际上是处理者。如果没有处理合同，且缺乏该类合同应包含的大部分条款，控制者就没有履行其义务。

温和的解释是："大多数专业人士不知道这一点"。严厉的解释是："不知法并不能免责"。而任何受咨询的数据保护专业律师的解释通常都是后者。

这具体对谁重要

对任何哪怕只是偶尔处理第三方个人信息的专业人士或公司都很重要：

- 接收客户资料（合同、诉状、声明、财产报告）的律师。
- 分享健康数据的医生和其他医疗专业人员——根据 GDPR 第 9 条，这些数据被视为具有强化保护制度的*特殊类别*。
- 处理身份、税务和银行数据的税务顾问和行政管理人员。
- 管理员工工作和个人资料的人事部门。
- 从潜在和现有客户处接收联系详情以及通常敏感的商业信息的商务代表。

在所有情况下，信息都受到 GDPR 的保护。在所有情况下，在通常的实践中，这些信息流经的渠道，其司法管辖权不允许在没有额外保证的情况下宣布其与欧洲框架"实质上等同"。这并非出于恶意。而是出于习惯。也是因为十五年来将便利置于合规之上的技术基础设施的结果。

"大家都在做"的论点

预见到最常见的反对意见是明智的："如果大家都在做，那就不可能是真正的问题"。这是一个完全可以理解的论点，但在法律上没有任何效力。一种做法普遍存在这一事实并不能使其符合条例。监管机构近年来已针对一些公司实施了处罚，原因正是那些在审计时刻之前看起来无害的即时通信使用方式。

目前的运营现实是，从可能性角度来看风险较低——监管机构很少会审计一家中型办公室的特定即时通信工具——但如果风险发生，从影响角度来看则是很高的。这是大多数人在不知道自己在承担风险的情况下所承担的风险。也就是说，没有评估所使用的工具是否符合数据控制者的法律责任。

数字足迹具有追溯力

还有第二个论点，与前一个几乎对称，值得预见："*如果这是一个严重的问题，行政部门早就开始监控了*"。目前观察到的现实在表面上证实了这一点。针对小公司尤其是自由职业者的即时通信违规使用检查目前几乎不存在——并不是因为这种行为被允许，而是因为大多数欧盟国家的行政部门缺乏审计数百万受义务实体所需的人力资源。

这就是目前观察到的实践所暗示的。但这并不是未来十年所暗示的。两个因素正在汇合，以在相对较短的时间内改变这种平衡。

第一：数字足迹具有追溯力。 通过带有中央服务器的应用发送的每条消息，至少在元数据中，会保留在持续存在的架构记录中。六个月前发送的内容在技术上今天仍然可以被审计。今天发送的内容在五年后仍然可以被审计。目前的监管缺位并不能保证未来的监管缺位。这是评估的推迟，而不是免除。

第二：行政审计能力将加速增长。 在监控流程中引入人工智能工具，消除了迄今为止（在事实上而非法律上）保护小公司和自由职业者的人力瓶颈。一个能够交叉比对大规模元数据、纳税申报、商业登记和安全漏洞通知义务的系统不需要督察员：它需要访问权限。而根据目前的监管框架，通过向在欧盟有法律存在的供应商提出要求来获得访问权限是完全可行的。

除此之外还有一个非技术但同样具有决定性的因素：欧洲国家正处于债务持续增长的过程中，几乎无一例外地需要扩大其税基。纯粹从财政角度来看，由于不遵守 GDPR 而产生的行政制裁是一个不断增长且在政治上方便的收入来源。这并非推测：这是欧洲数据保护机构年度报告中可观察到的趋势，罚款总额已连续多个财政年度上升。

对数据控制者的操作结论不是危言耸听，而是清醒的：**关于今天如何管理与客户沟通的决定，是根据发生检查那一年的审计能力来评估的，而不是根据现在的能力。** 而这种能力在合理的时间内将与今天有本质的不同。从今天开始正确做事的人不仅从今天起就没问题：从这一刻起生成的足迹将符合规范，这追溯性地保护了未来的这段时期。而像以前一样继续的人将积累可审计的足迹，其合规性将根据未来几年的标准和资源进行评估。

不同的架构会改变什么

存在不将数据存储在第三方基础设施中，而是直接从发送者设备传输到接收者设备的技术方案。在这种架构中，GDPR 关于国际传输的合规性不取决于标准合同条款，不取决于供应商的善意，也不取决于未来的审计。它取决于*没有传输*这一事实。而对于不存在的东西，就无法违规。

这并不是唯一的解决方案，也不是唯一可能的方案。但它在结构上是不同的，规范合规性不再是程序上的附件，而变成了设计的直接结果。对于认真对待其数据控制者责任的专业人士来说，这种区别至关重要。

下一期 Cuadernos 将详细分析 Schrems II 裁决及其对依赖美国云服务的初创公司及中小企业的实际影响，此时距该裁决发布已有五年。

来源及监管框架

- 条例 (EU) 2016/679 (GDPR)，特别是关于国际传输的第五章。
- 欧盟司法法院 C-311/18 (“Schrems II”)，2020 年 7 月 16 日。
- EDPB – 关于补充传输工具之措施的 01/2020 号建议。
- 数据保护机构 – 包含职业环境下即时通信使用不当处罚案例的年度报告。

← 上一页数字时代的职业秘密下一页 →当中间没有任何人时

最近阅读

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 27e212282bb1d03c88e6652291eb496a8540b33d7cb8394c485c9058423a9f3d

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。