分析 • 2026年5月26日

← 上一页 • 下一页 →

真实隐私与表面隐私：值得自问的那些问题

第二轮的实务综述：用以区分一项服务的隐私是架构性的还是宣示性的那些问题。一份供欧洲专业人士在为敏感数据采用任何数字工具之前使用的问卷。

把话说明白： 两项法律告知相同的服务，行事方式可能大相径庭。一项凭技术设计来保护。另一项凭合同承诺来保护。这一差别读告知是读不出来的——它是在提出具体问题时被发现的。答案的质量，与其内容本身一样能说明产品。

架构性隐私与宣示性隐私之别

在本轮此前的七篇文章中，我们走过了同一议题的不同层面。Schrems II 之下的国际传输之法。为每一本 Cuaderno 加封的密码学哈希这一数学构想。kill switch 这一架构选择，以及几乎总是与之相伴的机构俘获。端到端加密的机理，以及密钥存于何处这一实务之问。依商业模式而定的激励对齐。自主权式的密码学身份。作为相称策略的自托管。每一篇文章处理一个角度。本文，作为本轮的最后一篇，将它们汇聚成一份问卷。

值得记住的区分很简单：有些服务的隐私是*架构性的*，有些服务的隐私是*宣示性的*。前者嵌入于技术设计之中：对隐私承诺的某些违反，在技术上是困难的或不可能的，因为架构不允许它们发生。后者则寄托于法律告知的文字之中：某些违反一旦发生，在合同上是可被惩处的，但在技术上没有任何东西阻止它们。两种模式都能满足 GDPR；但一种凭构造来保护，另一种凭承诺来保护，而这一差别在实务上极为巨大。

接下来的问题，旨在将一种情形与另一种区分开来。它们并非高深的技术问题。它们是任何诚实的提供方都能在其公开文档中作答的问题。答案的质量与精确度，与答案本身一样能说明产品。这些问题归为六层；在为敏感数据采用服务之前，宜将它们悉数提出，而不只是第一直觉所辨识出的那几个。

第1层：架构

在继续之前，先界定一个术语。这里所说的 *operador* 指的是提供服务的公司——控制服务器和软件的主体，而非某个具体的人。明确这一点之后，根本的架构问题是：operador 对发送者与接收者之间的内容做了什么？可能的答案有三种，值得学会加以区分，因为这三种有时会用相似的措辞来宣传。

- 第一种：内容以明文经过 operador 的服务器，在那里 operador 即便承诺不读，也能读取它。

- 第二种：内容以加密形式经过 operador 的服务器，若密钥仅驻留于用户的设备之中，则 operador 无法读取它。
- 第三种：内容不经过 operador 的任何服务器，因为在那一具体的数据流中并不存在 operador 的服务器。

这三者之间的差别不是程度之别：而是种类之别。

与之互补的问题——已在关于加密的那本 Cuaderno 中提出——是：谁持有得以读取内容的加密密钥？若用户、且只有用户持有它，加密便是真实的。若 operador 也以任何形式持有它——哪怕是以「账户恢复」或「设备间同步」之名——加密便只是名义上的。这一问题不容许诚实的折中答案。

第2层：商业模式

关于商业模式的问题，其重要程度不亚于架构之问，且出于同一实质性的理由：激励会随着时间推移，系统性地产出不同的产品，纵然所宣示的宗旨完全相同。operador 今天如何赚钱？是单一来源、两种，还是混合？若资金来源包含广告或数据变现，哪些数据被变现，又是基于 GDPR 的哪一法律依据进行的？法律告知中所宣示的目的，是否涵盖专业人士打算托付给该服务的第三方数据？

还有那个并非总会被提出的二阶问题：operador 在三到五年后的财务状况如何？一家处于风险资本阶段的公司，所受的压力不同于一家处于稳定盈利的公司。融资模式的变更，一再地，正是与用户之间那份隐含契约在未经协商之下被重写的时刻。

第3层：司法管辖

对欧洲的专业人士而言，司法管辖之问绝非修辞。operador 在哪个司法管辖区注册成立？处理数据的服务器实际位于哪个国家？前述两问的答案是相同还是不同，若不同，适用哪国法律？一个由美国公司运营的欧洲区域，就 Schrems II 而言，并非一个欧洲的答案：无论服务器位于何处，该公司都受制于 FISA 702。

与之互补的实务之问是：倘若明天有一项在 operador 司法管辖区内有效的情报命令到来，要求交出我的数据或我客户的数据，会发生什么？若诚实的答案以「该公司将有义务交出它们」开头，那么无论广告如何暗示相反，该服务都无法抵御那道命令。若诚实的答案以「该公司无法交出，因为它并不以明文持有它们」开头，那么该服务确实能够保护；而这一差别几乎全然取决于前两层，而非隐私政策的质量。

第4层：operador 与 kill switch

operador 保留着哪些用以远程暂停、封锁、删除或降级服务的技术能力？这一问题并非杞人忧天：它是实务性的。数字平台近年来已反复行使该能力，有时出于自身的主动，有时是依政府命令，有时是在所有权或政策变更之后。若该能力确实存在，宜了解它在合同所声明的哪些前提下行使，并为那些未声

明的前提保留余地——近年来的实践已表明这些前提同样重要：出乎意料的司法命令、国际制裁、公司治理的变更、被另一家政策不同的实体收购。

与之相伴的问题是连续性计划：倘若 operador 对专业人士行使该能力——无论出于何种理由，正当与否——还会有多少可用时间，存在何种数据导出程序，又能迁移至哪一家替代提供方？若答案以「这本不该发生」开头，那便不是实务性的答案，而是一句承诺。

第5层：身份与访问

谁掌控服务的访问凭据？若 operador 能在用户不参与的情况下重置用户的访问权——这一程序通常被称为「账户恢复」——那么 operador 在技术上便是账户的保管者，也能够通过适当程序将其转交给提出请求的任何人。若 operador 因身份以密码学方式驻留于用户的设备而无法重置访问权，那么 operador 也就无法转交它，即便在命令之下亦然。这两种方式依语境皆属正当；但它们再一次有所不同，宜知晓自己正在采用的是哪一种。

倘若专业人士失去访问权，其数据会怎样？是否存在依赖于 operador 的恢复机制——账户的、文件的、会话的？若 operador 被胁迫使用这些机制，它们是否与该行业的职业伦理相容？

第6层：未来

这最后一层常被忽视，因为它要求前瞻。倘若该服务被另一家公司收购，会发生什么？几乎所有的收购，都会在随后数月内伴随服务条款的修订。倘若监管要求发生变化，会发生什么？欧洲法自 2022 年以来增加了下架与封锁的义务，而非减少。倘若 operador 消失了，会发生什么？相当一部分云服务并无针对 operador 关停这一情形而有据可查的退出计划；专业人士发现这一问题时，已无时间为之准备。

对于这一层，有一个值得记住的表述：越是较少依赖 operador 的架构，越能从容应对 operador 的变化。任何形式的自托管、自主权式的密码学身份、中间无服务器的通信，凡此种种，都通过减少当下的依赖面这一办法，来减少未来的风险面。它们并不消除风险；而是减少风险。

结构与承诺之别

倘若我们必须将本轮提炼为一句话，那便是：结构性的答案，纵使 operador、行政机关或法律发生变更，仍能维持；承诺式的答案，则只在作出承诺者尚能且尚愿维持之时维持。两者在采用之时都可能是正确的。但其中只有一种，能够不受时光流逝与情势变迁的左右而站得住脚。

这并不意味着每位专业人士都必须向其采用的所有服务索求结构性的答案。相称性依然正当：一份用于内部记账的电子表格，所需的答案不必与一名患者的诊疗档案相同。它的确意味着：所谓专业，就在于知晓自己在每一种情形下接受的是哪一类答案，并已有意识地判定该类答案与那项具体数据是相称的。

整理后的问卷

十二个综述本轮的具体问题，按使每一个的答案为下一个提供信息的方式排序：

1. 内容是否经过 operador 的服务器？若经过：是明文，还是以 operador 的密钥加密，抑或以用户专属的密钥加密？
2. 若声称采用端到端加密，加密密钥存于何处？operador 是否以任何形式知晓或保留其中任何一部分，包括以「恢复」之名？
3. 该服务生成并保留哪些元数据？保留多久？对谁可见？
4. operador 如何获得资金？若资金来源包含广告或数据变现，所宣示的目的是否涵盖专业人士所托付的第三方数据？
5. operador 在三到五年后的财务状况如何？是否存在某些因素，暗示其模式即将变更（待上市、行将耗尽的融资轮、可能发生的收购）？
6. operador 在哪个司法管辖区注册成立？服务器实际位于哪个国家？若两者不同，对处理适用哪国法律？
7. 倘若一项在 operador 司法管辖区内有效的情报命令要求交出我的数据，会发生什么？该公司在技术上能否予以执行？
8. operador 保留着哪些用以暂停、封锁或删除服务的技术能力？依据哪些合同所设定的前提？依据哪些历史上有据可查的、合同之外的前提？
9. 倘若 operador 不论正当与否地对我行使该能力，存在何种退出计划？是否有将数据导出至替代提供方的、有据可查的程序？
10. 谁掌控访问凭据？operador 能否在没有我参与的情况下重置它们？这是在保护我，还是在使我暴露？
11. 针对这一具体功能，是否存在欧洲的、自托管的，或中间无服务器的替代方案？与所评估的风险相比，它的真实成本是多少？
12. 倘若今天的决定在五年后被一位检查员、一位审计师，或一位因数据泄露而受损的客户加以审视，当下的选择能否凭今天可得的论据加以辩护，还是需要为未曾提出合理的问题而致歉？

这些问题并不期待完美的答案。它们期待诚实的答案——诚实的 operador 懂得作答，而不那么诚实的 operador 则回避精确地表述。两类 operador 之间的实务差别，我们不带戏剧化地说，往往在尚需进一步追问之前，便能通过细读他们自愿给出的答案而被察觉。

以本文，我们为 Cuadernos Lacre 的第二轮画上句号。我们以从 Schrems II 继承而来的编辑欠债开篇，以一份实务问卷收尾。一路上我们走过了若干概念——哈希、加密、身份——以及若干应用分析——kill switch、商业模式、自托管。本刊所宣示的编辑意图，并非以一份详尽无遗的问题清单去压垮读者，而是交给他一件工具，使他在面对任何新服务时，能分辨出自己正在接受的是哪一类答案。这种分辨——介于架构与承诺之间——便是那件工具。其余的，每位专业人士都会将其用于他在自身实务中认为值得这一问的数据。

来源及延伸阅读

- 本刊，第二轮（2026 年 5 月）——*Schrems II，五年后*、*SHA-256 究竟是什么*、*自毁开关 (Kill switch) 与机构俘获*、*真正讲清楚端到端加密*、*商业模式作为信任的信号*、*24 个单词：什么是加*

密身份、作为专业实践的自托管。本问卷所依托的七篇文章。
- 条例（欧盟）2016/679——《通用数据保护条例》。本问卷所提出的全部问题的参照法律框架，尤其是第 5、6、25、28、32、33 条以及第五章。
- 欧洲数据保护委员会——关于 Schrems II、国际传输、影响评估与主动问责的实务性指南与意见（2020-2024 年的出版物）。
- 西班牙数据保护局——2022-2024 年间公布的、针对因使用不当的传输工具，或因作出徒具形式而无实质内容的影响评估的数据控制者的处罚。
- noyb.eu——由 Maximilian Schrems 领导的欧洲数字权利中心。一个关于对欧洲数据保护规范之真实遵守（而非表面遵守）的投诉、申诉与分析的公开资料库。

← 上一页作为专业实践的自托管 (Self-hosting)下一页 →签名无法解决的问题

最近阅读

- 反思 · 2026年6月29日 你并不匿名
- 思考 · 2026年5月27日 签名无法解决的问题
- 分析 · 2026年5月25日 作为专业实践的自托管 (Self-hosting)

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 141ac1ba7d23b9590b7e97f3524e06d9ef90352e16dbaa0fb05695c93273837f

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