Analyse · 26. Mai 2026

← Zurück·Weiter →

Echte vs. scheinbare Privatsphäre: die Fragen, die man sich stellen sollte

Operative Synthese des zweiten Zyklus: die Fragen, die einen Dienst mit architektonischer Privatsphäre von einem mit deklarativer Privatsphäre unterscheiden. Ein Fragebogen für den europäischen Berufstätigen, bevor er ein digitales Werkzeug für sensible Daten einsetzt.

Damit wir uns verstehen: Zwei Dienste mit denselben Rechtshinweisen können sich sehr unterschiedlich verhalten. Der eine schützt durch technisches Design. Der andere schützt durch vertragliches Versprechen. Der Unterschied ist nicht in den Rechtshinweisen zu lesen — er wird entdeckt, indem man die konkreten Fragen stellt. Die Qualität der Antworten sagt ebenso viel über das Produkt aus wie ihr eigener Inhalt.

Der Unterschied zwischen architektonischer und deklarativer Privatsphäre

Im Verlauf der sieben vorangegangenen Artikel dieses Zyklus haben wir verschiedene Schichten desselben Themas durchschritten. Das Recht der internationalen Datentransfers mit Schrems II. Die mathematische Idee des kryptografischen Hashs, der jeden Cuaderno versiegelt. Die architektonische Wahl des Kill Switch und die institutionelle Vereinnahmung, die ihn fast immer begleitet. Den Mechanismus der Ende-zu-Ende-Verschlüsselung und die operative Frage, wo die Schlüssel liegen. Die Ausrichtung der Anreize gemäß dem Geschäftsmodell. Die selbstsouveräne kryptografische Identität. Das Self-Hosting als verhältnismäßige Strategie. Jeder Artikel befasste sich mit einem Blickwinkel. Dieser, der letzte des Zyklus, fasst sie in einem Fragebogen zusammen.

Die Unterscheidung, die man festhalten sollte, ist einfach: Es gibt Dienste, deren Privatsphäre *architektonisch* ist, und Dienste, deren Privatsphäre *deklarativ* ist. Die erste ist in das technische Design eingebettet: Bestimmte Verletzungen der Privatsphäre-Verpflichtung sind technisch schwierig oder unmöglich, weil die Architektur sie nicht zulässt. Die zweite ist im Text der Rechtshinweise hinterlegt: Bestimmte Verletzungen wären vertraglich sanktionierbar, falls sie geschehen, aber technisch hindert sie nichts daran. Beide Modelle können die DSGVO erfüllen; aber das eine schützt durch Bauweise und das andere durch Versprechen, und der Unterschied ist operativ enorm.

Die folgenden Fragen sind darauf ausgelegt, den einen Fall vom anderen zu unterscheiden. Es sind keine fortgeschrittenen technischen Fragen. Es sind die Fragen, die jeder ehrliche Anbieter in seiner öffentlichen Dokumentation beantworten kann. Die Qualität und Präzision der Antwort sagt ebenso viel über das Produkt aus wie die Antwort selbst. Die Fragen gruppieren sich in sechs Schichten; man sollte sie alle stellen, bevor man den Dienst für sensible Daten einsetzt, nicht nur die, die der erste Instinkt erkennt.

Schicht 1: Architektur

Halten wir vorab einen Begriff fest. Mit *Betreiber* meinen wir das Unternehmen, das den Dienst bereitstellt: die Instanz, die die Server und die Software kontrolliert, und keine konkrete Person. Damit geklärt, lautet die

architektonische Grundfrage: Was macht der Betreiber mit den Inhalten zwischen Absender und Empfänger? Es gibt drei mögliche Antworten, und man sollte sie unterscheiden können, denn alle drei werden mitunter mit ähnlichem Vokabular beworben.

- Die erste: Der Inhalt läuft über einen Server des Betreibers im Klartext, wo der Betreiber ihn lesen kann, auch wenn er verspricht, es nicht zu tun.
- Die zweite: Der Inhalt läuft verschlüsselt über einen Server des Betreibers, wo der Betreiber ihn nicht lesen kann, sofern die Schlüssel ausschließlich auf den Geräten der Nutzer liegen.
- Die dritte: Der Inhalt läuft über keinen Server des Betreibers, weil es in diesem konkreten Fluss keinen Server des Betreibers gibt.

Der Unterschied zwischen diesen dreien ist kein Gradunterschied: Es ist ein Artunterschied.

Die ergänzende Frage — bereits im Cuaderno über Verschlüsselung formuliert — lautet: Wer hat die kryptografischen Schlüssel, die das Lesen des Inhalts ermöglichen? Wenn der Nutzer sie hat und nur der Nutzer, ist die Verschlüsselung echt. Wenn der Betreiber sie zusätzlich in irgendeiner Form hat — selbst unter dem Namen «Kontowiederherstellung» oder «Synchronisierung zwischen Geräten» —, ist die Verschlüsselung nominell. Die Frage lässt keine ehrliche Zwischenantwort zu.

Schicht 2: Geschäftsmodell

Die Frage nach dem Geschäftsmodell ist ebenso wichtig wie die architektonische Frage, und aus demselben substanziellen Grund: Anreize bringen im Laufe der Zeit systematisch verschiedene Produkte hervor, selbst bei identisch erklärten Zwecken. Wie verdient der Betreiber heute Geld? Eine einzige Quelle, zwei, eine Mischung? Wenn die Finanzierung Werbung oder die Monetarisierung von Daten umfasst: Welche Daten werden monetarisiert und auf welcher Rechtsgrundlage der DSGVO geschieht das? Deckt der in den Rechtshinweisen erklärte Zweck die Daten Dritter ab, die der Berufstätige dem Dienst anzuvertrauen beabsichtigt?

Und die Frage zweiter Ordnung, nicht immer formuliert: Wie ist die finanzielle Lage des Betreibers auf Sicht von drei bis fünf Jahren? Ein Unternehmen in der Risikokapitalphase operiert unter anderen Zwängen als ein Unternehmen mit stabiler Rentabilität. Der Wechsel des Finanzierungsmodells ist wiederholt der Moment, in dem der implizite Vertrag mit den Nutzern ohne Verhandlung neu geschrieben wird.

Schicht 3: Gerichtsbarkeit

Für den europäischen Berufstätigen ist die Frage der Gerichtsbarkeit nicht rhetorisch. In welcher Gerichtsbarkeit ist der Betreiber eingetragen? In welchem Land stehen die Server physisch, die die Daten verarbeiten? Ist die Antwort auf die beiden vorigen Fragen dieselbe oder eine andere, und wenn sie sich unterscheidet, welches Recht gilt? Eine von einem US-amerikanischen Unternehmen betriebene europäische Region ist für die Zwecke von Schrems II keine europäische Antwort: Das Unternehmen unterliegt FISA 702 unabhängig davon, wo die Server stehen.

Die ergänzende operative Frage lautet: Wenn morgen eine in der Gerichtsbarkeit des Betreibers gültige nachrichtendienstliche Anordnung käme, die die Herausgabe meiner Daten oder der meiner Kunden verlangte, was würde geschehen? Wenn die ehrliche Antwort mit «das Unternehmen wäre verpflichtet, sie herauszugeben» beginnt, schützt der Dienst nicht gegen diese Anordnung, so sehr die Werbung auch das Gegenteil suggeriert. Wenn die ehrliche Antwort mit «das Unternehmen könnte sie nicht herausgeben, weil es sie nicht im Klartext hat» beginnt, schützt der Dienst sehr wohl; und der Unterschied hängt fast vollständig von den ersten beiden Schichten ab, nicht von der Qualität der Datenschutzerklärung.

Schicht 4: Betreiber und Kill Switch

Welche technische Fähigkeit behält der Betreiber, um den Dienst aus der Ferne auszusetzen, zu sperren, zu löschen oder herabzustufen? Die Frage ist nicht paranoid: Sie ist operativ. Die digitalen Plattformen haben diese Fähigkeit in den letzten Jahren wiederholt ausgeübt, mal aus eigenem Antrieb, mal auf Anordnung von Regierungen, mal nach Eigentümer- oder Politikwechseln. Wenn die Fähigkeit besteht, sollte man wissen, unter welchen vertraglich erklärten Voraussetzungen sie ausgeübt wird, und einen Spielraum für die nichterklärten Voraussetzungen reservieren, die sich in der Praxis der letzten Jahre als ebenso relevant erwiesen haben: unerwartete gerichtliche Anordnung, internationale Sanktion, Wechsel der Unternehmensführung, Übernahme durch eine Einheit mit anderer Politik.

Die Schwesterfrage ist die nach dem Kontinuitätsplan: Wenn der Betreiber die Fähigkeit gegen den Berufstätigen ausübte — aus welchem Grund auch immer, berechtigt oder nicht —, wie viel Betriebszeit bliebe verfügbar, welches Verfahren zum Datenexport besteht und zu welchem alternativen Anbieter könnte man migrieren? Wenn die Antwort mit «das sollte nicht passieren» beginnt, ist sie keine operative Antwort; sie ist ein Versprechen.

Schicht 5: Identität und Zugang

Wer kontrolliert die Zugangsdaten zum Dienst? Wenn der Betreiber den Zugang des Nutzers ohne dessen Beteiligung zurücksetzen kann — ein typischerweise «Kontowiederherstellung» genanntes Verfahren —, ist der Betreiber technisch der Verwahrer des Kontos und kann es auch demjenigen übergeben, der es über das geeignete Verfahren beantragt. Wenn der Betreiber den Zugang nicht zurücksetzen kann, weil die Identität kryptografisch auf dem Gerät des Nutzers liegt, kann der Betreiber sie auch nicht übergeben, nicht einmal auf Anordnung. Beide Modalitäten sind je nach Kontext legitim; aber, noch einmal, sie sind verschieden, und man sollte wissen, welche man gerade einsetzt.

Was geschieht mit den Daten des Berufstätigen, wenn dieser den Zugang verliert? Gibt es Wiederherstellungsmechanismen — für Konto, Datei, Sitzung —, die vom Betreiber abhängen? Sind diese Mechanismen mit der Berufsdeontologie der Branche vereinbar, wenn der Betreiber zu ihrer Nutzung gezwungen wird?

Schicht 6: Zukunft

Diese letzte Schicht wird oft vernachlässigt, weil sie eine Projektion erfordert. Was würde geschehen, wenn der Dienst von einem anderen Unternehmen übernommen würde? Fast alle Übernahmen ziehen in den folgenden Monaten eine Überarbeitung der Nutzungsbedingungen nach sich. Was würde geschehen, wenn sich die regulatorischen Anforderungen änderten? Das europäische Recht hat die Pflichten zur Entfernung und Sperrung seit 2022 erhöht, nicht verringert. Was würde geschehen, wenn der Betreiber verschwände? Ein erheblicher Teil der Cloud-Dienste hat keinen dokumentierten Ausstiegsplan für das Szenario der Betreibereinstellung; der Berufstätige entdeckt das Problem, wenn keine Zeit mehr bleibt, es vorzubereiten.

Es gibt eine Formulierung, die man für diese Schicht festhalten sollte: Architekturen, die weniger vom Betreiber abhängen, sind widerstandsfähiger gegenüber Veränderungen des Betreibers. Das Self-Hosting in jeder seiner Modalitäten, die selbstsouveräne kryptografische Identität, die Kommunikation ohne Server dazwischen — all dies verringert die künftige Risikofläche durch das Verfahren, die gegenwärtige Abhängigkeitsfläche zu verringern. Sie beseitigen sie nicht; sie verringern sie.

Der Unterschied zwischen Struktur und Versprechen

Müssten wir den Zyklus in einen einzigen Satz destillieren, wäre es dieser: Die strukturellen Antworten halten, auch wenn sich der Betreiber, die Verwaltung oder die Gesetzgebung ändern; die Antworten per Versprechen halten, solange derjenige, der verspricht, sie halten kann und will. Beide können im Moment ihrer Annahme richtig sein. Nur eine der beiden hält unabhängig vom Lauf der Zeit und vom Wandel der Umstände stand.

Das bedeutet nicht, dass jeder Berufstätige von allen Diensten, die er einsetzt, strukturelle Antworten verlangen müsste. Die Verhältnismäßigkeit bleibt legitim: Eine Tabellenkalkulation für die interne Buchhaltung braucht nicht dieselbe Antwort wie die Krankenakte eines Patienten. Es bedeutet aber, dass Professionalität darin besteht, zu wissen, welche Art von Antwort man in jedem Fall akzeptiert hat, und bewusst entschieden zu haben, dass diese Art von Antwort dem konkreten Datum angemessen ist.

Der Fragebogen, geordnet

Zwölf konkrete Fragen, die den Zyklus zusammenfassen, so geordnet, dass die Antwort auf jede die nächste informiert:

1. Läuft der Inhalt über einen Server des Betreibers? Wenn ja: im Klartext, mit Schlüsseln des Betreibers verschlüsselt oder mit ausschließlich dem Nutzer gehörenden Schlüsseln verschlüsselt?
2. Wenn Ende-zu-Ende-Verschlüsselung geltend gemacht wird: Wo befinden sich die kryptografischen Schlüssel? Kennt oder bewahrt der Betreiber einen Teil davon in irgendeiner Form, einschließlich der «Wiederherstellung»?
3. Welche Metadaten erzeugt und bewahrt der Dienst? Wie lange? Für wen sind sie sichtbar?
4. Wie finanziert sich der Betreiber? Wenn die Finanzierung Werbung oder die Monetarisierung von Daten umfasst: Deckt der erklärte Zweck die vom Berufstätigen anvertrauten Daten Dritter ab?
5. Wie ist die finanzielle Lage des Betreibers auf Sicht von drei bis fünf Jahren? Gibt es Faktoren, die auf einen unmittelbar bevorstehenden Modellwechsel hindeuten (anstehender Börsengang, auslaufende Finanzierungsrunde, wahrscheinliche Übernahme)?
6. In welcher Gerichtsbarkeit ist der Betreiber eingetragen? In welchem Land stehen die Server physisch? Wenn sie sich unterscheiden: Welches nationale Recht gilt für die Verarbeitung?
7. Was würde geschehen, wenn eine in der Gerichtsbarkeit des Betreibers gültige nachrichtendienstliche Anordnung die Herausgabe meiner Daten verlangte? Könnte das Unternehmen ihr technisch nachkommen?
8. Welche technische Fähigkeit behält der Betreiber, um den Dienst auszusetzen, zu sperren oder zu löschen? Unter welchen vertraglichen Voraussetzungen? Unter welchen historisch dokumentierten nichtvertraglichen Voraussetzungen?
9. Welcher Ausstiegsplan besteht, falls der Betreiber diese Fähigkeit gegen mich ausübte, zu Recht oder zu Unrecht? Gibt es ein dokumentiertes Verfahren zum Export der Daten zu einem alternativen Anbieter?
10. Wer kontrolliert die Zugangsdaten? Kann der Betreiber sie ohne meine Beteiligung zurücksetzen? Schützt mich das oder setzt es mich aus?
11. Gibt es für diese konkrete Funktion eine europäische, selbstgehostete oder serverlose Alternative? Wie hoch sind ihre tatsächlichen Kosten im Vergleich zum bewerteten Risiko?
12. Wenn die heutige Entscheidung in fünf Jahren von einem Inspektor, einem Auditor oder einem von einer Datenpanne betroffenen Kunden geprüft würde, wäre die jetzige Wahl mit den heute verfügbaren Argumenten vertretbar, oder erforderte sie eine Entschuldigung dafür, keine vernünftigen Fragen gestellt zu haben?

Die Fragen erwarten keine perfekten Antworten. Sie erwarten ehrliche Antworten, die der ehrliche Betreiber zu geben weiß und die der weniger ehrliche Betreiber vermeidet, präzise zu formulieren. Der operative Unterschied zwischen den beiden Arten von Betreibern, das sagen wir ohne Dramatik, lässt sich meist durch langsames Lesen der Antworten erkennen, die sie freiwillig anbieten, noch bevor man um mehr bitten muss.

Mit diesem Artikel schließen wir den zweiten Zyklus der Cuadernos Lacre ab. Wir begannen mit der von Schrems II ererbten redaktionellen Schuld und enden mit einem operativen Fragebogen. Auf dem Weg haben wir Konzepte durchschritten — Hash, Verschlüsselung, Identität — und angewandte Analysen — Kill Switch, Geschäftsmodell, Self-Hosting. Die erklärte redaktionelle Absicht der Publikation war nicht, den Leser mit der erschöpfenden Liste der Probleme zu überfordern, sondern ihm Werkzeuge an die Hand zu geben, damit er bei jedem neuen Dienst unterscheidet, welche Art von Antwort er gerade akzeptiert. Diese Unterscheidung —

zwischen Architektur und Versprechen — ist das Werkzeug. Den Rest wird jeder Berufstätige in den Dienst der Daten stellen, die er in seiner Praxis der Frage für würdig hält.

Quellen und weiterführende Literatur

- Diese Publikation, Zyklus 2 (Mai 2026) — *Schrems II, fünf Jahre später*, *Was SHA-256 wirklich ist*, *Kill Switch und institutionelle Vereinnahmung*, *Ende-zu-Ende-Verschlüsselung, wirklich erklärt*, *Das Geschäftsmodell als Vertrauenssignal*, *Die 24 Wörter: Was eine kryptografische Identität ist*, *Self-Hosting als berufliche Praxis*. Die sieben Artikel, auf denen dieser Fragebogen ruht.
- Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung. Rechtlicher Bezugsrahmen für alle Fragen, die der Fragebogen aufwirft, insbesondere die Artikel 5, 6, 25, 28, 32, 33 und das Kapitel V.
- Europäischer Datenschutzausschuss — operative Leitlinien und Stellungnahmen zu Schrems II, internationalen Datentransfers, Folgenabschätzungen und proaktiver Rechenschaftspflicht (Veröffentlichungen 2020-2024).
- Spanische Datenschutzbehörde — veröffentlichte Sanktionen 2022-2024 gegen Verantwortliche der Verarbeitung wegen ungeeigneter Transferinstrumente oder wegen formaler Folgenabschätzungen ohne substanziellen Inhalt.
- noyb.eu — Europäisches Zentrum für digitale Rechte, geleitet von Maximilian Schrems. Öffentliches Repositorium für Beschwerden, Rechtsmittel und Analysen zur tatsächlichen, nicht scheinbaren Einhaltung der europäischen Datenschutzvorschriften.

← ZurückSelf-Hosting als berufliche PraxisWeiter →Was eine Unterschrift nicht in Ordnung bringen kann

Aktuelle Lektüre

- Reflexion · 29. Juni 2026 Du bist nicht anonym
- Reflexion · 27. Mai 2026 Was eine Unterschrift nicht in Ordnung bringen kann
- Analyse · 25. Mai 2026 Self-Hosting als berufliche Praxis

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 67fc5e83915275a565e8bddf1e55e6a6b36f6d0f0994e1e420a1e40a77d20a28

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.