

Das Open Privacy Standard (OPS) Manifest

Ein globales, freies Metrik-System für digitalen Datenschutz und technologische
Mündigkeit

Ein Vorschlag für die globale Netzgemeinschaft

25. Februar 2026

Zusammenfassung

Die derzeitige Handhabung von Nutzerdaten durch globale Technologiekonzerne sowie die zunehmenden Bestrebungen staatlicher Überwachung untergraben das Grundrecht auf digitale Privatsphäre. Bestehende Lösungen wie die DSGVO oder ISO-Zertifizierungen versagen in der Praxis, da sie für den Endnutzer intransparent, bürokratisch und binär sind. Dieses Manifest skizziert den **Open Privacy Standard (OPS)**: Ein universelles, dezentrales Zertifizierungssystem, das Datenschutzqualität wie eine physikalische Maßeinheit behandelt und Software in eine leicht verständliche, fälschungssichere Notenskala (ähnlich dem Nutri-Score) einteilt. Begleitet von einer manipulationssicheren Prüfarchitektur zwingt der OPS den Markt durch radikale Transparenz zur Umkehr.

1 Status Quo: Das Scheitern der bisherigen Systeme

Wir befinden uns in einer Epoche, in der Daten das wertvollste Gut der Welt sind. Unternehmen wie Meta, Google oder Datenbroker haben Geschäftsmodelle perfektioniert, die auf der totalen Durchleuchtung des Individuums basieren. Parallel dazu wachsen staatliche Begehrlichkeiten: Gesetze zur Vorratsdatenspeicherung, Chatkontrolle oder Telekommunikationsüberwachung verlangen den systematischen Einbau von Schwachstellen in Rechenzentren. Wer absolute Verschlüsselung fordert, wird oft mit dem Totschlagargument konfrontiert: „*Wer nichts zu verbergen hat, hat auch nichts zu befürchten.*“

Dieses Argument ist fundamental falsch. Privatsphäre ist kein Indiz für Kriminalität, sondern die Grundvoraussetzung für eine freie, demokratische Gesellschaft. Wir verschließen unsere

Haustüren und nutzen Briefumschläge nicht, weil wir kriminell sind, sondern weil wir ein Recht auf einen unbeobachteten Raum haben.

1.1 Warum bestehende Alternativen versagen

Es mangelt nicht an Datenschutzgesetzen oder IT-Zertifikaten. Warum also ist das Problem nicht gelöst?

1. **Die Illusion der DSGVO / GDPR:** Gesetze wie die DSGVO sind wichtig, haben aber in der Praxis zu einer Flut an unlesbaren Cookie-Bannern und 50-seitigen Datenschutzerklärungen geführt. Der Nutzer klickt aus Erschöpfung auf „Akzeptieren“. Die Transparenz ist gescheitert.
2. **Die Binärität von ISO/SOC 2 Zertifikaten:** Wenn ein Unternehmen nach ISO 27001 zertifiziert ist, beweist das lediglich, dass es IT-Sicherheitsprozesse dokumentiert hat. Es bedeutet *nicht*, dass die Daten nicht verkauft werden. Zudem sind solche Zertifikate binär (bestanden / nicht bestanden). Sie bieten keine Abstufungen.
3. **Das Monopol-Problem:** Bisherige Prüfsiegel gehören oft einzelnen Organisationen, die Gebühren verlangen und nach eigenen, oft undurchsichtigen Kriterien werten.

2 Die Lösung: Der Open Privacy Standard (OPS)

Was wir brauchen, ist keine neue Behörde und kein neues Monopol, sondern eine **Idee**, ein freies Protokoll. Der *Open Privacy Standard* adaptiert die Erfolgsmechanismen der Open-Source-Community (wie GPL-Lizenzen) und überträgt sie auf den Datenschutz.

Der OPS trennt die Definition des Standards von den Prüfern. Der Standard definiert eine Maßeinheit (ähnlich dem physikalischen „Meter“ oder den „Schulnoten“). Jeder kann diese Metrik nutzen, lesen und verstehen. Unabhängige Prüffirmen konkurrieren auf dem freien Markt darum, Unternehmen nach genau dieser offenen Metrik zu prüfen.

2.1 Das Ökosystem des Vertrauens

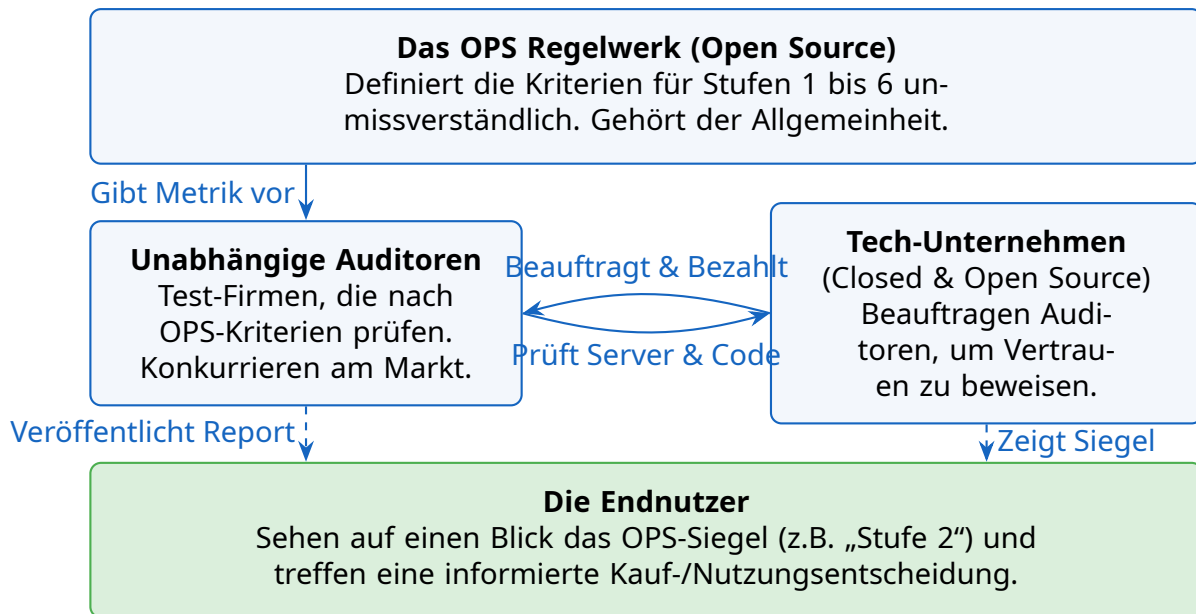


Abbildung 1: Architektur und Datenfluss des Open Privacy Standards

3 Die Metrik: Das OPS-Stufensystem

Das Herzstück des OPS ist seine radikale Einfachheit für den Endnutzer. Eine Software darf keine Kompromisse eingehen, um eine Stufe zu erreichen. Erfüllt ein Unternehmen alle Kriterien für Stufe 2, scheitert aber an einem einzigen Punkt, fällt es gnadenlos auf Stufe 3 oder tiefer zurück.

Stufe	Bezeichnung	Bedingungen (Auszug)
1	Absolut (The Gold Standard)	Keine personalisierte Datenspeicherung. Nutzung von verschlüsseltem Rechnen (Confidential Computing/Zero-Knowledge). Niemand, auch nicht das Unternehmen oder staatliche Akteure, kann Daten mitlesen. Quellcode ist vollständig Open Source.
2	Fairer Kompromiss	Daten werden gesammelt, aber niemals an Dritte verkauft oder weitergegeben . Nutzung der Daten ausschließlich für unternehmenseigene Zwecke. Nachweisliche und garantierte Löschung aller Daten nach einer festen Frist (z.B. 6 Monate). Quellcode darf Closed Source sein, wird aber durch Auditoren technisch tiefen-geprüft.
3	Befriedigend	Daten werden nicht verkauft, aber zur Profilbildung innerhalb eines Ökosystems genutzt und dauerhaft gespeichert. Server stehen in Ländern mit strikten, bewiesenen Datenschutzgesetzen.
4	Ausreichend	Nutzung von standardisierten Drittanbieter-Diensten (z.B. Google Analytics) ist vorhanden. Daten verlassen das Unternehmen, jedoch nur in anonymisierter Form.
5	Mangelhaft	Daten werden an Partnerunternehmen oder Datenbroker weitergegeben. Intransparente Speicherfristen.
6	Ungenügend (Status Quo)	Das Unternehmen verdient sein Geld hauptsächlich mit dem unregulierten Verkauf von Nutzerprofilen. Keine verifizierbare Löschung. Implementierte staatliche Hintertüren (Backdoors).

4 Anti-Korruption: Wie man Bestechung verhindert

Eine der kritischsten Schwachstellen jedes Zertifizierungssystems ist der Interessenskonflikt: Der Prüfer wird von dem Unternehmen bezahlt, das er prüfen soll. Wie verhindert der OPS, dass sich Milliardenkonzerne einfach eine „Stufe 2“ kaufen?

Der OPS löst dieses Problem durch **Krypto-ökonomische Anreize und radikale Transparenz**:

1. **Der offene Audit-Report (Das Paper):** Ein OPS-Siegel ist ohne den dahinterliegenden technischen Bericht wertlos. Wenn Firma X das Siegel Stufe 2 erhält, muss der Auditor

den vollständigen Prüfbericht (Welche Datenbanken wurden geprüft? Wie funktioniert das Lösch-Skript? Welche Traffic-Analysen wurden gemacht?) öffentlich zugänglich machen.

2. **Das "Peer-Auditing" (Audit the Auditor):** Hier greift das Bug-Bounty-Prinzip. Wenn Test-Firma A einem Unternehmen die Stufe 2 bescheinigt, kann Test-Firma B (die Konkurrenz) diesen offenen Bericht analysieren. Findet Firma B heraus, dass Firma A schlampig gearbeitet hat oder bestochen wurde (z.B. weil doch Daten abfließen), meldet sie dies.
3. **Drakonische Konsequenzen:** Fliegt ein falsches Gutachten auf, verliert der betroffene Auditor sofort seine Akkreditierung im OPS-Netzwerk. Sein Geschäftsmodell ist vernichtet. Die entdeckende Test-Firma erhält hingegen Reputations-Boni. Dies erzeugt ein systemisches Misstrauen *zwischen* den Auditoren, was die Integrität des Siegels für den Endnutzer sichert. Es ist lukrativer, Fehler der Konkurrenz aufzudecken, als sich von einem Konzern bestechen zu lassen.

5 Die Technologische Konsequenz: Der Schutz der Gesellschaft

Eine häufige politische Kritik an Systemen, die wie OPS-Stufe-1 aufgebaut sind (End-to-End-Verschlüsselung, Keine Logs, Schweizer Server), lautet, dass sie Geheimdiensten und Ermittlungsbehörden die Arbeit erschweren. Dies ist unbestreitbar richtig. Eine Architektur, die nicht abgehört werden *kann*, kann von niemandem abgehört werden – weder von Hackern, noch von Werkkonzernen, noch vom Staat.

Doch dieses Gesetz der Mathematik ist kein Bug, es ist ein Feature. Der OPS vertritt die philosophische Haltung, dass der Schutz der zivilen Infrastruktur, der Industrie und der Millionen von unbescholtenen Bürgern vor Datenlecks, Identitätsdiebstahl und Überwachungskapitalismus ein ungleich höheres Gut ist, als die theoretische Bequemlichkeit von Ermittlungsbehörden.

Wenn Staaten per Gesetz (z.B. durch TKÜ-Schnittstellen in deutschen Rechenzentren) Backdoors fordern, zwingen sie Unternehmen automatisch in die OPS-Stufen 3 bis 6. Das OPS-Siegel macht diesen politischen Eingriff transparent. Wenn ein deutsches Unternehmen seinen Nutzern erklären muss, dass es wegen nationaler Gesetze maximal Stufe 4 erreichen kann, entsteht ein massiver politischer und wirtschaftlicher Druck auf den Gesetzgeber, diese Überwachungs-gesetze zu reformieren, um die heimische Wirtschaft im globalen Wettbewerb nicht zu benachteiligen.

6 Fazit

Wir müssen das Narrativ umkehren. Nicht der Nutzer muss beweisen, warum er Privatsphäre will, sondern die Industrie muss transparent beweisen, dass sie dieses Vertrauen verdient. Der Open Privacy Standard ist mehr als ein Konzept; er ist ein Instrument zur Rückeroberung der di-

gitalen Mündigkeit. Er entzieht der Datenschutz-Debatte die juristische Komplexität und macht sie zu einer einfachen, knallharten Metrik, an der kein Unternehmen mehr vorbeikommt.

Die Umsetzung erfordert keine staatliche Erlaubnis. Sie erfordert lediglich eine Gemeinschaft, die den Standard definiert, und erste wagemutige Prüf-Firmen und Softwareunternehmen, die dieses neue Zeitalter des Vertrauens einläuten.